SECURITY RESOURCE GROUP INC.

SRG Policy and Procedures Manual

Updated: May 21, 2020

SRG Security Resource Group Inc.

300 – 1914 Hamilton Street
Regina, SK S4P 3N6
Ph: 306-522-0135
Fax: 306-352-4110

May 21, 2020

To: All SRG Employees

From: Blair Ross, President & COO

Re: Policy & Procedures Manual

The following Policy and Procedures Manual is for the use of SRG Security Resource Group Inc. (SRG) employees in carrying out your functions to ensure a safe and efficient working environment for all. It is intended to be a "living" general policy document that will be updated as policies and processes change to better SRG.

This manual provides for corporate policies and procedures for various functions in SRG. It is important that you read and understand the policies as they are designed for your safety and to provide quality service for our clients.

Whether expressly written or not, the policies apply to both SRG employees and/or contractors acting on behalf of SRG.

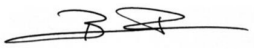
Collective Agreements (if applicable) and various Provincial Legislations may have additional and/or modified information with respect to some policies in this general policy manual. In that event the applicable Collective Agreement or Provincial Legislation takes precedent.

Not every activity may have a policy associated with it. It is the responsibility of every employee to act in accordance with the intent of the polices and make good judgements if something is not specifically covered in this manual.

SRG employees working on/for clients, on sites and/or systems, will also be required (in some instances) to follow the policies of the client in addition to the SRG Policies. Specifics will be provided in Standing Orders (or by other communication) to ensure you have the information required. This is intended to ensure we are delivering the service expected at a client's site in a safe and professional manner.

If you have any questions, please direct them to your supervisor for clarification. Should you have no questions we will accept that as you have read, understood and agreed to adhere to the policies.

Sincerely,
SRG Security Resource Group Inc.



Blair W. Ross
President & COO

Table of Contents

CODE OF CONDUCT

1000.10 Basic Standards

Effective Date:	**June 29, 2012**
Last Updated:	**April 20, 2020**
Approved By:	**Blair Ross**

Purpose

It is recognized that no written code of conduct can cover every situation; rather, the standards of conduct set out in this Code are stated in broad terms, indicating the general direction and rules by which conduct should be measured.

Scope

This policy applies to all employees and contractors acting on behalf of SRG.

Policy

All personnel will comply with the Basic Standards at all times.

Procedure

All personnel should in all of their actions, be guided by and demonstrate the following:

- At all times, comply with the law and avoid any activity which breaches any applicable law (federal, provincial and municipal).
- Act with honesty and integrity.
- In dealings with others, respect differences in ideas and opinions and avoid public confrontations or disputes.
- Respect and treat others fairly and with dignity and courtesy, regardless of their race, ancestry, place of origin, colour, ethnic origin, citizenship, religion, gender, sexual orientation, age or disability.
- Be in control of their actions at all times.
- Take responsibility for their actions.

Change History

April 20, 2020 - Added contractors acting on behalf of SRG

1000.20 Core Values

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

The core values are the principles that SRG has identified to guide the behaviours of all persons associated with SRG and its subsidiaries.

Scope

This policy applies to all staff.

Policy

The core values adopted by SRG describe how SRG's directors, officers and employees should act in order to accomplish SRG's mission.

SRG's Core Values are as follows:

- INTEGRITY: We strive to ensure that we deliver appropriate solutions for our clients' needs.
- EXCELLENCE: We are committed to provide the best quality, value, service and results to our clients.
- VISION: We are committed to being highly creative, innovative and future-orientated in providing solutions to our clients.
- WELLNESS: We strive to promote individual and corporate health and wellness for our clients and ourselves at the physical, emotional, mental and spiritual levels.
- TRUSTWORTHINESS: We provide sound expertise that can be relied on.
- RESPECT FOR OTHERS: In our approach to problems, we are careful to honour the worth of all people.
- RESPECTABILITY: We value earning the reputation as leaders in our areas of expertise.
- HONESTY: A high degree of ethical business and personal behaviour guides all our endeavours.

Change History

<Summarize changes to the previous version.>

1000.25 Off-Duty Conduct

Effective Date:	**April 24, 2020**
Last Updated:	**April 24, 2020**
Approved By:	**Blair Ross**

Intent

The purpose of this policy is to outline the expectations for SRG employees regarding off-duty conduct. Off-duty conduct may have a serious effect on business interests and the workplace in general and as such SRG will enforce the guidelines of this policy. If it is shown that there is a connection between an employee's off-duty conduct and the workplace, disciplinary action may be taken.

Guidelines

When employees are off-duty there is still an expectation by SRG that employees will conduct themselves in a way that positively represents the company's values and mission statement.

Off-duty conduct of employees may be subject to disciplinary action up to and including termination if it is shown that:

- the conduct of the employee harms SRG's reputation, product or business interests;
- the employee's behaviour renders the employee unable to perform his/her duties satisfactorily;
- the employee's behaviour leads to refusal, reluctance or inability of the other employees to work with him/her;
- the employee has been guilty of a serious breach of the Criminal Code and thus rendering his/her conduct injurious to the general reputation of SRG and its employees;
- the employee's behaviour places difficulty in the way of SRG properly carrying out its function of efficiently managing its works, and efficiency directing its working forces.

Disciplinary action will be taken if any one of these criteria is met.

An investigatory process will be followed in order to determine the validity and severity of the incident and the resulting disciplinary actions.

False or Frivolous Complaints

Employees should be cognizant of the fact that a formal accusation against another employee is a serious allegation with repercussions.

Where allegation of inappropriate off-duty conduct is found to be either false or frivolous, or where supporting documentation for a complaint has been falsified, the complainant or witness may be subject to disciplinary measures up to and including termination of employment.

Change History

<Summarize changes to the previous version.>

1000.30 Confidential Information

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

The success of SRG depends on its competitiveness, and it is the creation and possession of timely and accurate information, which allows us to compete.

Scope

This policy applies to all staff.

Policy

Confidential information about company business, affiliated companies, customers or competitors gained from your affiliation with SRG shall not be discussed or disclosed with anyone outside the company. In addition to guarding against deliberate disclosure, you must also be vigilant about unintended disclosure. Exercise the utmost caution in all public places and refrain from discussing confidential business in, for example, elevators, restaurants, bars, airplanes.

Procedure

Failure to comply with this policy may result in disciplinary action, including termination.

Change History

<Summarize changes to the previous version.>

1000.40 Conflict of Interest

Effective Date:	**June 29, 2012**
Last Updated:	**April 20, 2020**
Approved By:	**Blair Ross**

Intent

SRG continually strives to protect our business interests from real or potential conflicts of interest, and has adopted this policy to outline procedures for avoiding and reporting various situations where a conflict of interest may arise.

Guidelines

The Transaction of Business

Employees should avoid:

- Any interest, investment or association that creates a conflict of interest or that interferes with their ability to perform their duties with SRG; and
- The creation of any personal direct or indirect interest or relationship with any company that competes with or provides products and/or services to SRG.

Additionally, where a situation arises where an employee is required to conduct business or provide services to a family member, or associate, this may create a real or perceived conflict of interest for both the company and the employee in question.

Where our resources (including property, equipment and personnel) are used for unapproved purposes, they may create a negative impact on our business, and the community perception of the company. SRG strictly prohibits the use of personnel (including volunteers) and/or equipment for non-company business, as their use may be improper, illegal or create a conflict of interest.

If any employee has reason to believe that a conflict of interest has occurred or is possible, it is their duty to report it to management.

Outside Employment

SRG generally allows outside employment where:

- The secondary employment causes no adverse effects on the employee's performance of job duties with us;
- The secondary work is performed after the employee's regularly scheduled working hours with us; and
- The outside employment is not in direct competition with SRG
- There is no conflict of interest.

Any employee that wishes to work part-time, or for any amount of time after their regularly scheduled work hours with us should discuss the matter with his/her Manager prior to accepting the secondary employment. The employee may be required to disclose information pertaining to the proposed secondary employment to allow a full review. The review will simply ensure that there is no conflict of interest.

Situations where a SRG employee is required to conduct business or provide services to a family member or associate may create a real or perceived conflict of interest for both the company and the employee in question. As such, SRG requires any employee who feels he/she may have a conflict of interest to immediately notify his/her Manager for relief.

If any SRG employee has reason to believe that a conflict of interest has occurred or is possible, it is his/her duty to report it to management. SRG strictly prohibits any retaliation for fulfilling this obligation.

Conflict of Interest in Hiring Practices

Family Members

- SRG can accept applications from, and consider a member of an employee's immediate family for employment if the candidate has all the requisite qualifications.
- An immediate family member shall not be considered for employment if by doing so, it might create a direct or indirect managerial/subordinate relationship with the family member, or if his/her employment could create a conflict of interest either real or imagined.
- For the purposes of this policy, immediate family members shall be defined as: Wife, Husband, Mother, Father, Brother, Sister, Son, Daughter, or any In-Laws.
- Approval for the hiring of a family member of any employee is to be made by the President & COO.

Employee Relationships

- SRG employees involved in romantic relationships, or that become married or live in the same household shall not be perceived as presenting a conflict of interest, provided that there is neither a direct or indirect managerial/subordinate relationship between the employees, or a conflict of interest, real or perceived, created as a result of the relationship.
- In the event that either a managerial/subordinate, or conflict of interest issue arises, SRG will work with the employees to accommodate them in a reasonable fashion. Possible resolutions resulting from a conflict of interest may require one of the employees to transfer to another department or position within the company. If this is not possible, one of the employees may be required to resign.

Reporting a Conflict of Interest

Employees

Employees who believe they have witnessed a conflict of interest, or where they reasonably believe that they may be engaged in any activity which could present a conflict of interest must report the matter immediately. SRG must be made aware of all conflicts of interest in order to take the appropriate action. Employees are obligated to report any conflict of interest to their immediate supervisor, manager or the President & COO.

Supervisors & Managers

Supervisors and managers are directed to take all appropriate steps to prevent and stop conflicts of interest in their areas of responsibility. Any supervisor or manager who is subject to, witnesses, or is given written or verbal complaints of conflict of interest shall work to minimize or eliminate the issue at hand. In the event that this is not possible with the available resources, the supervisor / manager is required to report the conflict of interest to the President & COO.

Investigation

SRG seeks to resolve claims of conflicts of interest as expediently as possible. Investigations shall be conducted and the appropriate actions taken no longer than (30) days following the filing of a complaint.

In all cases, the President & COO shall retain the findings report for any administrative or legal action arising out of the complaint is pending.

Assurance Against Retaliation

This policy encourages employees to report any conflict of interest encountered in their employment at SRG. Retaliation against the Complainant is strictly prohibited and will result in appropriate disciplinary action. Retaliation

by the Respondent, or anyone acting on behalf of the Respondent, against any witness providing information about a conflict of interest report, is also strictly prohibited. Acts of retaliation include (but are not limited to) interference, coercion, threats, and restraint.

This policy will not be used to bring fraudulent or malicious complaints against employees. Any complaint made in bad faith, if demonstrated as being such through convincing evidence, will result in disciplinary action being taken against the individual lodging the fraudulent or malicious complaint.

Change History

April 20, 2020 - Details on hiring of family members
April 20, 2020 - Further details on complaint and investigation processes.

1000.50 Code Breach Complaint Resolution

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

Complaints of breaches of this Code by SRG personnel may arise. The objective of SRG in this process is to uphold its core values as described in this Code.

Scope

This policy applies to all employees of SRG.

Policy

The investigation of a complaint will involve all normal processes of a thorough and fair examination of the facts and will provide an opportunity for all affected parties to bring forward relevant information. Conclusions reached as a result of the investigation will be reported in writing to the President & COO, as may be applicable to the personnel involved.

Procedure

Complaints of breaches of this Code will be investigated at the direction of SRG's President & COO, or in the case of a complaint involving the President & COO, at the direction of the Chair of the Board.

Either such party may delegate the investigation of a complaint, as circumstances may dictate. In the normal course, in order for SRG to act on a complaint it should be in writing and signed by the complaining party and reasonable evidence regarding the validity of the complaint shall be available. The objective of SRG in determining whether a complaint should be investigated will simply be to do its best to achieve fairness between the personnel in respect of whom the complaint is made, and the complaining party, so as to eliminate complaints which, are for example, based solely on hearsay, are of a purely personal nature or otherwise do not properly require a response under this code.

After receiving the result of the complaint investigation, the President and COO will determine whether and what action should be taken regarding the accused personnel or situation in general. Action in this regard may include a direction regarding counselling or other remedial action, a reprimand, a suspension or termination of employment.

SRG will take action where it considers it appropriate to do so whether the circumstances arise by virtue of a complaint from a member of the public or supplier or, whether SRG otherwise determines that such action is necessary.

Change History

<Summarize changes to the previous version.>

GENERAL OPERATIONS

2000.08 Substance Abuse Policy

Effective Date:	**January 1, 2014**
Last Updated:	**October 11, 2018**
Approved By:	**Blair Ross**

Purpose

SRG is committed to the health and safety of its employees and has adopted this policy to communicate its expectations and guidelines surrounding substance use, misuse, and abuse.

Employees under the influence of drugs or alcohol on the job can pose serious health and safety risks to both themselves and their fellow employees. To help ensure a safe and healthy workplace, SRG reserves the right to prohibit certain items and substances from being brought on to or present on company premises.

Scope

This policy applies to all SRG employees (and contractors working on behalf of SRG) while they are engaged in company business, working on company premises or worksites, and operating company vehicles and equipment.

Policy

Definitions

Drug: Any substance which can change or adversely affect the way a person thinks or feels, whether obtained legally or illegally. This could include recreational cannabis, cocaine, opiates, and amphetamines.

Drug paraphernalia: Material or equipment used or intended for use in injecting, ingesting, inhaling, or otherwise introducing a drug, illegal or controlled, into the human body.

Medication: Includes a drug obtained legally, either over the counter or through a prescription issued by an authorized medical practitioner. For this policy, medications of concern are those that inhibit a worker's ability to perform their job safely and productively.

Alcohol: Any beverage containing any quantity of alcohol, including, beer, wine, and distilled spirits.

Expectations

The following expectations apply to employees and management alike while conducting work on behalf of the company, whether on or off company property:

- Employees are expected to arrive to work fit for duty and able to perform their duties safely and to standard;
- Employees must remain fit for duty for the duration of their shift;
- Use, possession, distribution, or sale of drugs or alcohol during work hours, including during paid and unpaid breaks, is strictly prohibited;
- Employees are prohibited from reporting to work while under the influence of recreational cannabis and any other non-prescribed substances;
- Use and possession of medically prescribed drugs is permitted during working hours, subject to the terms and conditions of the company's policies and all applicable legislation;
- Employees on medically approved medication must communicate to management any potential risk, limitation, or restriction requiring modification of duties or temporary reassignment; and

- Employees are expected to abide by all governing legislation pertaining to the possession and use of cannabis.

Procedure

Roles and Responsibilities

SRG will:

- Clearly communicate expectations surrounding alcohol and drug use, misuse, and abuse;
- Maintain a program of employee health and awareness;
- Provide a safe work environment; and
- Review and update this policy regularly.

Management will:

- Identify any situations that may cause concern regarding an employee's ability to safely perform their job functions;
- Ensure that any employee who asks for help due to a drug or alcohol dependency is provided with the appropriate support (including accommodation) and is not disciplined for doing so; and
- Maintain confidentiality and employee privacy.

Employees must:

- Abide by the provisions of this policy and be aware of their responsibilities under it;
- Arrive to work fit for duty, and remain so for the duration of their shift;
- Perform work safely in accordance with established safe work practices;
- Avoid the consumption, possession, sale, or distribution of drugs or alcohol on company property and during working hours (even if off company property);
- When off duty, refuse a request to come into work if unfit for duty;
- Report limitations and required modifications as a result of prescription medication;
- Report unfit co-workers to management;
- Seek advice and appropriate treatment, where required;
- Communicate dependency or emerging dependency to management or human resources

Suspicion of Impairment

The following procedure may be enacted if there is reasonable belief that an employee is impaired at work:

1. If possible, the employee's manager or supervisor will first seek another manager's or supervisor's opinion to confirm the employee's status.
2. Next, the manager or supervisor will consult privately with the employee to determine the cause of the observation, including whether substance abuse has occurred. Suspicions of an employee's ability to function safely may be based on specific personal observations. If the employee exhibits unusual behaviour including but not limited to slurred speech, difficulty with balance, watery or red eyes, or dilated pupils, or if there is an odour of alcohol, the employee should not be permitted to return to their assigned duties in order to ensure their safety and the safety of other employees or visitors to the workplace.
3. If an employee is considered impaired and deemed "unfit for work," this decision is made based on the best judgement of two members of management and DOES NOT require a breathalyzer or blood test. The employee may be advised that SRG has arranged a taxi or shuttle service to safely transport them to their home address or to a medical facility, depending on the determination of the observed impairment. The employee may be accompanied by a manager or supervisor or another employee if necessary.

4. An impaired employee will not be allowed to drive. The employee should be advised if they choose to refuse SRG organized transportation and decide to drive their personal vehicle, the company is obligated to and will contact the police to make them aware of the situation.
5. A meeting may be scheduled for the following work day to review the incident and determine a course of action which may include a monitored referral program as part of a treatment plan.

Possession at Work

Possession of alcohol, drugs, and drug paraphernalia on company property is prohibited. Company property encompasses all company (and its clients) owned or leased property used by employees, including without limitation parking lots, vehicles, lockers, desks, and closets.

Possession of alcohol, drugs, and drug paraphernalia is also prohibited while employees are acting on behalf of the organization off of company (or its clients) premises. This includes attending events as a company representative.

Disciplinary Action

Employees may be subject to disciplinary action up to and including termination of employment for failure to adhere to the provisions of this policy, including but not limited to:

- Failure to meet prescribed safety standards as a result of impairment from alcohol or drugs; and
- Engaging in illegal activities (for example, selling drugs or alcohol while on company premises).

Additional Information

Substance Dependency

SRG understands that certain individuals may develop a chemical dependency to certain substances, which may be defined as a disease or disability. Employees are not excused from their duties as a result of their dependencies. SRG promotes early diagnosis. Any employee who suspects that they might have an emerging drug or alcohol problem is expected to seek appropriate treatment promptly.

The company will work with the individual who requests accommodation in an effort to ensure that the measures taken are both effective and mutually agreeable, up to the point of undue hardship. Employees are encouraged to communicate any need for accommodation to their immediate supervisor, and to work with them in addressing the concern.

Voluntary Identification

Employees are encouraged to communicate if they have a dependency or have had a dependency so that their rights are protected and they can be accommodated appropriately. Employees will not be disciplined for requesting help or due to current or past involvement in a rehabilitation effort.

All medical information will be kept confidential by SRG, unless otherwise authorized by law.

Medical Cannabis

Where an employee uses medical cannabis, it is expected they provide a copy of their medical documentation for use SRG and abide by the company's accommodation policy.

Agreement for the Continuation of Employment

SRG reserves the right to invoke an agreement for the continuation of employment in accordance with an employee's commitment to become and remain alcohol- and drug-free. The agreement will outline the conditions governing the employee's return to the job and the consequences for failing to meet the conditions.

An agreement for the continuation of employment may include a requirement for drug or alcohol testing.

Change History

Updates and renames Policy 2000.08 (Alcohol & Drug Policy) due to the legalization of Cannabis in Canada effective October 17, 2018.

2000.09 Medical Cannabis Policy

Effective Date:	**April 24, 2020**
Last Updated:	**April 24, 2020**
Approved By:	**Blair Ross**

Intent

The employees of SRG are our most valuable resource, and for that reason their health and safety are of paramount concern. Medical cannabis will be treated the same as any regularly prescribed medication. SRG has the same expectations from employees who use medical cannabis as those who use all other types of medication and will accommodate individuals up to the point of undue hardship.

Guidelines

- Employees may only use medical cannabis with appropriate documentation in their names from a qualified health care practitioner as defined by the *Access to Cannabis for Medical Purposes Regulations.*
- If an employee must use medical cannabis while at work and requires accommodation to do so, they must inform their supervisor/manager. An employee does not have to disclose their specific medical diagnosis; however, they must provide a note from their doctor and a copy of the appropriate documentation if accommodation is required.
- All information provided in regard to medical cannabis use is considered confidential and will be treated as such, keeping an employee's privacy as a top concern second only to safety.
- Employees who have a medical condition which requires additional accommodation can discuss their cannabis use schedule in the context of the general accommodation plan with SRG and their qualified health care practitioner.
- Employees may be required to work with the company's service provider, who will provide direction and support for the use of medical cannabis.
- SRG will work with the individual who requests accommodation to ensure that the measures taken are both effective and mutually agreeable.

Use of Medical Cannabis While at Work

- If an employee takes medical cannabis during regular working hours, they shall do so only at the recommended dosage and frequency of the doses.
- Where possible employees who require medical cannabis use a method of consumption other than smoking.
- Employees who choose to smoke medical cannabis must abide by all provincial, client and SRG smoking regulations.
- Employees who choose to smoke medical cannabis are not permitted to smoke in the presence of other employees.

Expectations

<u>Management must:</u>

- Treat employees who use medical cannabis the same as all other employees using prescription medication.
- Provide accommodation up to the point of undue hardship.
- Be aware of the effects of cannabis use and ensure employees are not placed in any safety-sensitive situations.
- Assess the effects of the use of cannabis on an employee's performance on the job.
- Ensure that the use of medical cannabis does not adversely affect the safety of the employee or their co-workers.

- Ensure that any employee who asks for help due to a drug or alcohol dependency is provided with the appropriate support (including accommodation) and is not disciplined for doing so.
- Respond to any employee queries regarding the use of medical cannabis, while maintaining the privacy of an employee's specific situation at all times.

Employees must:

- Work with SRG to develop accommodation plans that are mutually agreeable.
- Follow the agreed-upon accommodation plan and the guidelines of this policy.
- Never share their medication with any other employee, even those who may have a similar authorization.
- Maintain ongoing communication with management regarding the effects of cannabis on their ability to perform their job duties.
- Never participate in activities which could cause a safety risk, such as driving while under the influence of cannabis.

Change History

<Summarize changes to the previous version.>

2000.10 Asset Handling

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that employees will be given access to use assets of SRG and/or our clients'.

Scope

This policy applies to all SRG Employees

Policy

SRG employees who have access to SRG or Client assets (i.e. Laptops, flashlights, etc.) must ensure they are accounted for and properly maintained at all times. Assets not authorized for use by SRG employees must not be handled/used in any way.

Procedure

At the start of any shift the employee will verify that all assets are accounted for.

At the end of the respective shift the employee will ensure applicable assets have been turned in and are accounted for.

All applicable assets must be kept in a secure area when not in use.

The Operations Supervisor or Regional Manager will verify all assets are accounted for on a regular basis.

All asset counts must be recorded on paper and signed off by the SRG employee and/or manager who performed the count.

Change History

<Summarize changes to the previous version.>

2000.20 Blood/Bodily Fluid

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

To educate and make all employees aware of blood and certain body fluids should be considered a hazard for the potential of bloodborne pathogen infections. Employees should understand what pathogens may be present in certain body fluids and what is considered a "significant exposure."

Scope

This policy applies to all employees.

Policy

Supervisor Responsibility:

Supervisors must conduct a Risk Assessment of all jobs carried out by security staff and educate their staff on possible exposure to blood or body fluids and how to reduce the risk of infection in the event of a significant exposure.

Employee Responsibility:

There are a number of bloodborne pathogens of which Hepatitis B and C and HIV (AIDS) are the most important. Transmission occurs by direct contact with infected blood or certain other body fluids (e.g. semen, vaginal secretions, blood tinged body cavity fluids, etc.)

Exposure to feces, urine, vomitus, sputum, tears, nasal secretions are not considered risky unless visibly blood tinged. For workplaces where workers are exposed to sharp objects (e.g. knives, saws, scissors, needles), procedures for safe handling and first aid are required.

What is Significant Exposure?

Significant exposure to blood or body fluids where there is risk of infection happens only in certain ways:

- puncturing the skin with a sharp object coated with B/BF e.g. needle stick, razor, broken glass, scissors, knife, etc.
- splashing blood onto mucous membrane (eyes, nose, mouth)
- splashing blood onto non-intact skin (e.g. abrasion, eczema, other damaged skin)

Personal Protection

<u>Handwashing</u>

Handwashing is the most important aspect of infection control, regardless of the appropriate use of gloves. Hands must be washed thoroughly with soap and water after all direct contact with B/BF.

<u>Gloves</u>

Latex or vinyl gloves are to be worn when:

- handling any items soiled with B/BF
- in direct contact with B/BF

- in contact with open wounds or sores

Disposal of Gloves

Gloves should be disposed of in a separate garbage bag and not be placed into the regular garbage. Once gloves are separately bagged, they may be placed into regular garbage for disposal.

Respiratory Protection

Disposable devices with a one-way valve mechanism should be available for mouth to mouth cardiopulmonary resuscitation (CPR). All first aiders should carry this device at all times.

Procedure

When an exposure incident occurs:

1. Determine whether a significant exposure has occurred (see definition).
2. Get first aid immediately – flush thoroughly.
3. Report the incident to appropriate supervisors or occupational health personnel.
4. Seek medical attention immediately if a significant exposure occurred – preferably within two hours. Timely assessment is necessary for the initiation of preventative medication and/or vaccination.

Workplace Clean-up Procedures

AS A SECURITY PROFESSIONAL IT IS NOT YOUR RESPONSIBILITY TO PERFORM CLEAN-UP PROCEDURES. The following is for information purposes only:

Spills

Floor areas or benches contaminated with B/BF should be promptly cleaned with absorbent disposable paper towelling and then disposed of in plastic bags. The area should then be cleaned with water and detergent followed by disinfecting with household bleach, one part bleach to nine parts water (1:10 dilution), and allowed to air dry. If mops have been used in the cleanup, they should be thoroughly washed in soap and water and dried before re-use.

Soiled Clothing

Clothing soiled with B/BF should be removed and laundered in the usual fashion. Soiled Tools and Instruments Tools, chisels, drill bits, etc. which come into contact with B/BF should be cleaned with paper towels, washed and decontaminated with appropriate disinfectant.

Cleaning Products

Soap (and water) is the most common and most easily accessible cleaning product. A commonly used disinfectant is household bleach solution, one part bleach to nine parts water (1:10 dilution) prepared daily. For decontamination of aluminum or electronic equipment, use 70 per cent isopropyl alcohol solution and apply for 10 minutes.

Sharps Disposal Procedures

Safe pick-up procedures to be practised. Do not place in regular garbage. Safe garbage handling procedures are to be used.

NOTE:

- B/BF contact with intact skin is not considered to be a risk for the spread of bloodborne pathogens.

- Vaccination against Hepatitis B is highly recommended for workers at risk of exposure to B/BF in their usual duties.

Change History

<Summarize changes to the previous version.>

2000.25 Communications

Effective Date:	**April 29, 2020**
Last Updated:	**April 29, 2020**
Approved By:	**Blair Ross**

Purpose

The Communication Policy is intended to establish guidelines for the disclosure of SRG information. The disclosure of SRG's business information must be handled in a uniform and consistent manner, as it is critical to the ongoing success of the company and the way that SRG is perceived by the public.

This Communication Policy extends to all employees, supervisors, and managers at SRG at all times and without exception and covers all forms of communication, whether oral, written, or electronic (i.e., email, social media, etc.).

Scope

This policy applies to all SRG employees (and contractors working on behalf of SRG) while they are engaged in company business, working on company premises or worksites, and operating company vehicles and equipment.

Guidelines

SRG will work to ensure that the information provided to the public regarding the company is accurate, informative, and positive. As such, SRG will:

- Provide information regarding our products, services, and performance to the media and the public at large as appropriate;
- Appoint a designated media spokesperson to convey news o media outlets and respond to their inquiries;
- Provide a consistent source of information when posting news to any media format and when responding to inquiries; and
- Direct any media inquiries to the President & COO.
- The President/COO or the Chair/CEO are the only SRG employees authorized to make media statements on behalf of SRG.

Confidential Business Information

Regarding all communications, employees are required to verify with the President & COO whether the information can be shared with persons outside of the company. If an employee is in doubt about whether certain information should be shared, the employee should refrain from sharing any information until approval is received.

By establishing this restriction, SRG ensures that:

- A consistent message is delivered to the public regarding company matters; and
- The company controls the release of confidential information.

<u>Determination of Whether Information is Confidential</u>

Information about SRG is considered to be confidential if it has a significant effect or would reasonably be expected to have a significant effect on the community's regard or impression of the company.

SRG shall provide to all employees ongoing education on the importance of maintaining the confidentiality of company business information and the protocol to be followed in the event that they are asked (whether orally, in writing, or electronically) to comment on SRG's confidential business information.

Protection of Confidential Business Information

In order to ensure that SRG's confidential business information is protected, the following procedures should be observed:

- Confidential matters should not be discussed in places where the discussion may be overheard, such as elevators, hallways, restaurants, airplanes, or taxis.
- Confidential documents should not be read in public places and should not be discarded where others can retrieve them.
- Employees must ensure they maintain the confidentiality of information in their possession outside of the office.
- Transmission of documents by electronic means, such as by fax or directly from one computer to another, should be made only where it is reasonable to believe that the transmission can be made and received under secure conditions.
- Unnecessary copying of confidential documents should be avoided and documents containing confidential information should be promptly removed from conference rooms and work areas after meetings have concluded. Extra copies of confidential documents should be shredded or otherwise destroyed.
- Access to confidential electronic data should be restricted through the use of passwords.
- Documents and files containing confidential information should be kept in a safe place where access is restricted to individuals who need to know that information in the necessary course of business.
- All proprietary information, including computer programs and all files and their contents, remain the property of SRG and may not be removed, disclosed, copied, or otherwise used except in the normal course of employment or with the prior permission of the President & COO.

Electronic Communications

Employees are prohibited from participating in discussions about SRG on electronic chat rooms or newsgroups. Chat rooms or newsgroups may be the source of rumours about SRG, which may or may not be factual. Employees shall not respond to such rumours in the chat rooms, newsgroups, or social media sites. Employees should inform the President & COO if they encounter a discussion pertaining to SRG.

SRG Website and Web Links

SRG maintains a company website and will ensure that any data posted to the website is accurate and shows the date that it was posted (as applicable). The President & COO must authorize any posting of information to the company website. The website will be updated as necessary with new information or changes to any information.

Links from SRG's website to a third-party website must be approved by the President & COO. Any such links will include a notice that advises the reader that he or she is leaving SRG's website and that the company is not responsible for the contents of the other site.

Email Communications

Communication by email leaves a physical track of its passage that may be subject to later decryption attempts. All confidential information being transmitted over the internet must be secured by the strongest encryption and validation methods available.

Employees must be aware of potential issues and limitations in using email to transmit confidential information.

Electronic Inquiries

Response to electronic inquiries will be the responsibility of the President & COO. Only public information or information which could otherwise be disclosed in accordance with this policy shall be utilized in responding to electronic inquiries.

Rumours

If a rumour (whether from a chat room, newsgroup, or a non-electronic source) is circulating about SRG and employees become aware of it, employees are required to inform the President & COO so that the information may be refuted as necessary.

Responsibilities

SRG will ensure that:

- Communications between SRG and the general public are controlled as necessary;
- Employees are trained on the appropriate use and disclosure of confidential business information;
- Employees are aware of the identities of those responsible for communicating on behalf of SRG;
- All written, electronic, and oral disclosures are reviewed and approved before they are shared with the public;
- The company's website and social media sites are monitored for the disclosure of inappropriate information;
- This policy is updated regularly, as new developments occur;
- The effectiveness of and compliance with this policy are monitored; and
- Those violating this policy are subject to progressive discipline, up to and including termination of employment.

Change History

<Summarize changes to the previous version.>

2000.30 Conflict Resolution Policy

Effective Date:	**June 29, 2012**
Last Updated:	**April 20, 2020**
Approved By:	**Blair Ross**

Intent

SRG is committed to providing a workplace free of conflict, where employees are treated with fairness, dignity and respect. SRG has instituted this policy to provide employees with an outlet to raise concerns regarding any conflict in the workplace or dissatisfaction with respect to issues related to their employment in an open and fair manner with provisions made to ensure their prompt and reasonable resolution. Under no circumstance should any employee fear discrimination or reprisal in the workplace as a result of the filing of a complaint.

Guidelines

Conflicts

The following conflicts should be reported, and SRG shall strive to address them with reasonable resolutions:

- Disputes with co-workers or managerial staff with unwanted, and unresolved consequences.
- Perceived unfair or inequitable treatment.
- Harassment whether sexual, discriminatory, or personal in nature.
- Abuse of authority.
- Administration of company policies.

Conflict Reporting Procedure

Discussion

- Employees are encouraged to discuss the unwanted behaviour or actions with the offending party as the situation dictates.
- Under ideal circumstances, the two parties shall reach a reasonable resolution without the necessity of the filing of a formal complaint.
- In the event that a discussion is not feasible or fails to reach a reasonable resolution, a formal complaint may be filed.

Reporting

- Complainants should record the details of the unwanted circumstance(s), the names of any applicable witnesses, and any attempts made to resolve the issue heretofore.
- Formal complaints stemming from unresolved employee or managerial conflicts shall be submitted in writing with any pertinent documentation, to either you supervisor/manager, or Human Resources.
- Formal complaints shall be reviewed and investigated.
- Formal complaints must be submitted within 14 days from the date of the alleged incident(s).
- In all cases where formal complaints have been lodged, it is important to maintain a policy of strict confidentiality between the complainant and the responder (manager / HR). For investigative purposes, the offending party may be notified.
- Anonymous complaints shall not be reviewed.

Employee Expectations

Employees

1. Employees are required to fully comply with the Conflict Resolution Policy.
2. Shall be treated fairly throughout the process, as either a complainant, or alleged offending party.
3. Shall be responsible for maintaining confidentiality regarding their involvement, and the complaint itself.
4. Shall co-operate with any investigations in relation to complaints.

Management / Human Resources

- Management and Human Resources shall be responsible for enacting preventative measures to ensure a workplace that is free from harassment, and for the communication of policy and procedures contained herein.
- Management and Human Resources shall receive and address properly filed complaints in an appropriate fashion.
- In the event that the complainant and the offending party are engaged in a subordinate-supervisor relationship, they may be physically removed from each other on a temporary basis, and may require a change in their reporting relationship.
- Investigate, or co-investigate any complaints, claims and documentation therein.
- Attempt to reach a reasonable resolution to the conflict.
- Inform the complainant and the offending party of possible resolutions available.

Resolutions

- If an apology is made by the offending party, and the complainant accepts the apology, this may be viewed as a reasonable resolution.
- All attempts shall be made to reach a reasonable resolution through internal mediation of the complaint with both parties' involvement.

Where the complaint is substantiated:

In the event that a complaint is substantiated and a reasonable solution to halt the unwanted behaviour or action through mediation is not possible, the following actions shall be taken for the offending party:

- Written warning/reprimand.
- Transfer or demotion, and in some instances both a transfer and a demotion.
- Education and training.
- Suspension.
- Termination of Employment.

Where the complaint is not substantiated:

In the event that a complaint is not substantiated due to lack of evidence or other reasons, both parties shall be informed with the rationale used. The complainant shall be notified first.
Both parties should be reminded that an unsubstantiated complaint does not necessarily mean that it was filed under false or frivolous pretences.

A complainant may request that the investigation be re-opened in the event that pertinent new evidence can be provided, or a reprisal due to the allegation has occurred.

Records

SRG shall keep on file all formal complaints, and the accompanying documentation, and the findings of any investigation.

Information from a previous investigation resulting in a substantiated complaint may be used for review and consideration purposes in the event of a new allegation.

False or Frivolous Complaints

- Employees should be cognizant of the fact that a formal complaint against another employee is a serious allegation with repercussions.
- Where a complaint is found to be either false or frivolous, or where supporting documentation for a complaint has been falsified, the complainant or witness may be subject to disciplinary measures up to and including termination of employment.

Change History

April 20, 2020 – Addition details on the policy and the handling of complaints

2000.40 Progressive Discipline Policy

Effective Date:	**June 29, 2012**
Last Updated:	**April 20, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that an employee may not follow company and/or client policies. SRG uses progressive discipline to address performance, conduct, and policy violation issues. Progressive discipline allows employees to correct any issues or concerns and reduces the need for termination of employment. SRG strives to work with employees regarding any issues in the workplace but also needs to hold employees to a high standard of performance and conduct. Therefore, a progressive, multi-step disciplinary process has been implemented.

Scope

This policy applies to all SRG employees and contractors acting on behalf of SRG.

Policy

Disciplinary actions may result if an employee/contractor does not adhere to company/client policies.

Procedure

Employees will be given multiple opportunities to correct the identified issue or concern, unless the issue or concern is severe, in which case progressive discipline can be accelerated to match the violation. Typically, progressive discipline proceeds through these steps:

1. Coaching (informal);
2. Verbal warning (formal);
3. First written warning (formal);
4. Final written warning with possible suspension (formal); and
5. Termination.

With each violation or apparent problem, the employee will be provided with a written document to alert them of the problem and, if applicable, provide a copy of the company policy being violated; advise them of the consequences for further infractions; and suggest a method for improvement.

Informal Coaching

Before giving a formal verbal warning, SRG may provide employees with informal coaching. Informal coaching is a documented process that offers the employee an opportunity to correct an issue before starting the formal discipline process and receiving a verbal warning. Depending on the nature of the issue or concern, this step may be skipped.

Formal Warnings

All formal warnings will be kept on file for 24 months. If no further discipline occurs within the time period, the warning will become inactive. If further offences relating to the issue occur, the warning will be attached to the next set of progressive disciplinary actions.

Degrees of discipline will be used in relation to the problem at hand. As the situation dictates, based on the past performance of the employee and the seriousness of the violation, SRG reserves the right to skip the four-step disciplinary process and move straight to termination when necessary.

Investigation and Documentation

All alleged violations will be properly investigated and documented by a manager or human resources. All formal measures taken within the progressive discipline process will be documented and kept in the employee's personnel file.

Suspension

During the final written warning, an employee may be suspended or put on review. Employees put on suspension will be excluded, with pay, from the workplace for a period of one to three days, depending on the violation. Typically, suspension will be for three days unless the employee is required at work to complete projects or perform required duties. The purpose of the suspension will be to provide the employee time to reflect on their actions as well as their continued employment with SRG.

Termination of Employment

The final stage of progressive discipline is termination of employment. Termination of employment with SRG may occur following an employee committing multiple violations of company policy, after the logical steps for progressive disciplinary action have been taken, or immediately following a severe violation.

No employee shall be disciplined or discharged for refusal to work on a site or in any workplace where he/she has reasonable grounds to believe that it would be unsafe or unhealthy to do so or where it would be contrary to Federal, Provincial or Municipal legislation or regulations. In such circumstances, the employee must remain at or near the work site until an Occupational Health & Safety Inspector attends the site to give a determination.

All employee terminations must have the approval of an Executive in charge of the division prior to the termination taking place.

Change History

April 20, 2020 – added 1. Coaching to the progressive discipline and details of the various disciplines.

2000.50 Emergency Procedures

Effective Date:	**June 29, 2012**
Last Updated:	**October 1, 2013**
Approved By:	**Blair Ross**

Purpose

SRG recognizes the safety and wellbeing of employees could be in jeopardy if there are no emergency procedures in place.

It is the goal of SRG to be prepared for emergency situations should they arise. We will strive to have procedures for all foreseeable situations to avoid, panic, confusion, or incident during an emergency.

It is the responsibility of job site managers and supervisors to gather information such as the location of the nearest hospital, fire station, and first aid station, and qualified first aid personnel in order to minimize travel time to treatment for all employees. This information will be posted conspicuously on site for all to view.

All employees will be trained in the emergency procedures, roles and responsibilities and will follow the instruction set out by their supervisors in the event of an emergency.

SRG will activate an emergency DRILL without warning to test the emergency procedures for deficiencies, and to ensure all employees have an active and working knowledge of the emergency procedures. These drills will be held at minimum, once per calendar year. Deficiencies noted at the time of the drill including, evacuation efficiency and time, supervisor guidance, and visitor sign in will be documented to assist in improving our systems to mitigate inefficiencies.

Scope

This policy applies to all employees of SRG and any sub-contractor of SRG.

Policy

The client's emergency response plan will always prevail.

SRG's emergency response plan must be followed if (a) the client does not have an emergency response plan or (b) the client's emergency response plan is deemed inadequate by SRG management.

The client is responsible for providing a site-specific emergency response plan. SRG is responsible for providing appropriate training to all employees. Emergency response drills are to be performed on a regular basis.

Procedure

Evacuation procedures are approved by the customer and are incorporated into the Post Orders for all personnel. Prior to being assigned to a client site, all employees are trained for site-specific evacuation procedures and designated meeting spot(s). Site supervisors are responsible for ensuring all evacuees arrive safely to the designed evacuation meeting spot.

Evacuation Procedures:

1. Proceed to the nearest/designated exit immediately.
2. Go directly to the designated meeting spot.
3. Site supervisor will do a head count.
4. If someone is missing, site supervisor must report to authority immediately.
5. Remain at the designated spot until permission to leave is granted.

When evacuating a building or a site:

- DO NOT run.
- DO NOT panic.
- DO NOT gather personal items.
- DO NOT make phone calls.
- DO NOT yell or talk unnecessarily.
- DO NOT bring any food or beverage.

Certain measures are taken prior to the emergency or disaster to ensure an effective response. SRG employees are trained on the use of emergency equipment and the location thereof, alerting and notification systems, procedures and infrastructure protection. A map showing the emergency equipment locations is available to workers at the primary security post.

The emergency service that is called upon depends on the nature of the emergency. The means of communication to report an emergency is site specific. Call 911immediately if police, fire or EMS is needed. Every site must either have access to a cellular telephone or a two-way radio. A list of emergency contact numbers is available to workers at the primary security post if 911 is not needed. The emergency contact numbers list must be updated on a regular basis.

Emergency response drills are performed on a regular basis.

Change History

<Summarize changes to the previous version.>

2000.51 Communicable Disease and Illness Control

Effective Date:	**April 29, 2020**
Last Updated:	**April 29, 2020**
Approved By:	**Blair Ross**

Purpose

SRG has instituted this policy to create guidelines for communicable disease and illness control. The guidelines provided are designed to protect both clients and employees from contracting and/or spreading communicable diseases and illnesses. This policy must be used in conjunction with all applicable health and safety regulations and governmental legislation.

Scope

This policy applies to all SRG employees (and contractors working on behalf of SRG) while they are engaged in company business, working on company premises or worksites, and operating company vehicles and equipment.

Guidelines

Security Resource Group will comply with all requests and orders issues by Public Health Officials and its representatives. All employees will be provided with periodic general education on infection prevention and control (IPAC) practices. This education will include:

- The risks associated with communicable diseases;
- The importance of appropriate immunizations;
- Hand hygiene;
- Appropriate cleaning and/or disinfection of items;
- Any pertinent health notices that may affect the workplace; and
- Employee responsibilities in the face of health notices or bulletins.
- Employees must follow all health and safety policies at all times.

Notifiable Diseases

These diseases include, but are not limited to:

- Acquired Immunodeficiency Syndrome (AIDS)
- Chickenpox
- Congenital infections
- Foodborne illness
- Human Immunodeficiency Virus (HIV) infections
- Measles
- Meningitis
- Mumps
- Norwalk Virus
- Severe Acute Respiratory Syndrome (SARS)
- Tuberculosis

Employees Who May be Contagious

- Employees who may have contracted a communicable disease and are in the early stages of infection should not report to work as they may infect the others in the workplace.
- Employees who may be contagious should immediately self-isolate to prevent any possible spread of the infectious disease, and contact the local public health authority and follow their advice.

- Employees are required to exercise their judgement and call-in if they are contagious, using the Call-In Procedure.
- Management at SRG will keep records of absences due to illness and is responsible for noting any alarming trends or repeated outbreaks of infections. In any cases where a pattern is noted, senior management will be notified so that additional infection control procedures can be put into place where necessary.
- Employees should only return to the SRG or site workplace when they are no longer symptomatic or when a medical professional has certified that they are no longer contagious.

Outbreak or Significant Risk of Spread

In the event that there is an outbreak of a communicable disease or there is a significant risk of the spread of infection involving multiple individuals, SRG will take all reasonable precautions to protect its staff and clients, including a lockdown of the company premises if necessary, according to SRG's Influenza Pandemic Policy.

SRG will work in conjunction with health officials to ensure that the health and safety of all parties is adequately protected.

Transmission of Microorganisms

Employees and clients of SRG may be exposed to pathogenic microorganisms, bacteria, and other microbes that can cause infection and disease. Transmission of microorganisms can be caused by contact transmission from hands (direct) or objects (indirect), droplet transmission from coughing or sneezing, or airborne transmission from the inhalation of organisms surviving in air for long periods of time.

Other routes of entry for infection include:

- Injection;
- Inhalation;
- Ingestion; and
- Contact with the skin, eyes, or nose.

While it may not be possible for SRG to completely eliminate all routes of entry for infections, employees share a responsibility to follow safe work procedures and practices to mitigate the risk of infection.

Routine Practices

Following routine practices helps to protect both the employees and clients of SRG from pathogens. Consistent practices must be used at all times with all persons as someone could be infected but be asymptomatic.

Hand Hygiene

Hand hygiene is the most important measure in preventing the transmission of microorganisms. Hand hygiene includes both washing the hands with plain or antimicrobial soap with water as well as non-rinse alcohol-based hand rubs.

SRG will implement a hand hygiene program that incorporates the following elements:

- Provides employees with the ability to wash their hands with soap and water or alcohol-based hand rub when working with a client;
- Provides education to employees about how and when to wash their hands;
- Provides employees with hand moisturizer which is compatible with hand hygiene products to help maintain the skin's integrity; and
- Ensures that client hand hygiene is also supported.

Employees of SRG should wash their hands with soap and running water:

- If hands are contaminated with bodily fluids or visibly soiled, including when soiled with powder from hand protection gloves; and
- After any personal body function.

Employees should exercise good judgment when determining if hands should be washed. If it is possible that hands may have become contaminated with bodily fluids, they should be washed with soap and water or sanitized.

Additional Hand Hygiene Guidelines

- Hand hygiene should be done in a manner appropriate for the type of situation.
- Bar soap must never be used – instead, liquid soap should be provided in disposable pump dispensers.
- Soap dispensers should be discarded when empty and not refilled or topped-up.
- Hand lotion should never be petroleum-based as it may affect glove integrity.

Respiratory Etiquette

SRG expects that all employees practice respiratory etiquette and personal practices that help to prevent the spread of microorganisms and encourages clients to do the same. These personal practices include:

- Avoidance measures that minimize contact with droplets when coughing or sneezing, including:
- Turning the head away from others;
- Maintaining a two (2) metre distance from others;
- Covering the nose and mouth with a tissue. If tissues are not available, other avoidance measures (e.g., coughing or sneezing into sleeve) may be used;
- Immediate disposal of tissues after use; and
- Immediate hand hygiene after disposal of tissues.

Personal Protective Equipment (PPE)

PPE creates a physical barrier that protects an employee's own tissue from exposure to infectious materials and from transmission resulting from contact with clients. The type of PPE is dependent on the nature of the interaction with the client. Employees of SRG are to wear appropriate PPE when interacting with clients who may pose a risk of transmitting microorganisms. Common PPE includes gloves and facial protection.

Gloves

- As gloves may break, proper hand hygiene must be performed prior to putting on gloves.
- Gloves must always be changed if the employee is going from one client meeting to another.
- Gloves should be put on immediately before performing the activity for which they are being used.
- Gloves must be removed and discarded immediately after use; hand hygiene must then also be performed.
- Non-latex gloves must be used if a latex allergy is present for an employee or a client.
- Employees who have any open wounds on their hands are required to wear a bandage over the wound and then gloves over the bandage.

Facial Protection

- A mask can be used in the event that Health Canada recommends it for airborne infectious diseases.
- Masks should be put on immediately before the activity for which it is indicated, and hand hygiene is to be performed after removing the mask.

Environmental Cleaning and Sanitizing

Cleaning is the removal of foreign material (e.g., dust, soil, blood secretions, microorganisms, etc.). Cleaning physically removes rather than kills the microorganism and thorough cleaning is required for any equipment/surface to be disinfected, as organic matter may inactivate a disinfectant.

Disinfection is the process used on inanimate objects and surfaces to kill microorganisms. Cleaning and disinfecting agents may be combined into a single product to save a step in the cleaning and disinfecting process.

Maintaining a clean and healthy environment is integral to the safety of employees and clients and is a top priority at Security Resource Group. Environmental cleaning and disinfection are performed on a routine and consistent basis to provide a safe and sanitary environment.

Employee Immunizations

To protect both employees and clients, SRG expects employees to have (some/all) of the following immunizations:

- Annual influenza vaccine;
- Measles, mumps and rubella (MMR) vaccine (two (2) doses) or documentation of immunity;
- Tetanus vaccine (every 10 years).

Change History

<Summarize changes to the previous version.>

2000.52 Influenza Pandemic Planning

Effective Date:	**September 2, 2009**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG Security Resource Group Inc. (SRG) has adopted this policy to ensure the ongoing health and safety of our employees and to ensure business continuity in the event of an influenza pandemic or outbreak. All reference to this policy should be directed to Blair Ross, President and COO.

Scope

This policy applies to all SRG Employees.

Guidelines

The President & COO shall work with senior management following the planning guidelines outlined in this section. The goal of planning and coordination efforts is to provide leadership and coordination across sectors. One important aspect is to integrate pandemic preparedness into national emergency preparedness frameworks.

Periods and Phases

For help with response planning at SRG, please refer to the table of pandemic periods and phases (Table 1). These guidelines have been sourced from the World Health Organization (WHO).

Table 1- Pandemic Periods and Phases

Period	Description	WHO Phases
Inter-Pandemic Phase	New Virus in animals, no human cases	1 - 2
Level 1 - Pandemic Alert	New Virus causes human cases	3
Level 2 - Pandemic Warning	Evidence of increased human-to human transmission	4 - 5
Level 3 - Pandemic	Efficient and sustained human-to-human transmission Suspected/Confirmed case(s) in the Province	6
Level 4 - Pandemic	Confirmed case(s) at SRG or in the City	6
Post-pandemic Period	Return to inter-pandemic period	7

Suggested Actions

Level 1

- Review existing business continuity plans and/or develop pandemic-specific procedures as appropriate.
- Identify ways to promote prevention and identify ways to minimize staff, customer and visitor exposure and illness.
- Implement prevention and illness minimization plans/activities including Handwashing/Hygiene procedures and well as the clean office and facilities.
- Encourage employees to make sure that their immunizations are current and up to date. Suggest all employees to have their current flu shot.
- Consider how essential messages can be communicated across SRG.

- Establish mechanisms for alerting staff to a change in pandemic status.
- Establish procedures and triggers for escalating a response.
- Follow local Health authority guidelines – legislation

Level 2

- Alert staff to a change in pandemic status.
- Implement prevention and illness minimization plans/activities including Handwashing/Hygiene procedures and well as the clean office and facilities.
- Continue to encourage employees to make sure that their immunizations are current and up to date. Continue to suggest all employees to have their current flu shot.
- Initiate pandemic information communication activities.
- Activate international travel safety plans.
- Review/test business continuity plans.
- Follow local Health authority guidelines – legislation.

Levels 3 & 4

- Alert staff to the change in pandemic status.
- Activate measures to minimize introduction and/or spread of influenza (social distancing, management or tracking of illness, cancellations, closures, etc.)
- Activate essential business continuity measures and establish regular review and emergency management process.
- Review and update risk and impact assessment.
- Set response objective and identify specific action required.
- Determine and establish activities/services to be maintained or discontinued (who needs to come to work).
- Communications with staff regarding the SRG status and to promote confidence in the workplace and response activities.
- Activate the process for recovered/well staff members to return to work.
- Follow local Health authority guidelines – legislation.

Post-Pandemic Period

- Review and update risk and impact assessments.
- Establish criteria and process for agreeing to return to business normal.
- Activate process for communicating business normal status to staff, customers and visitors.
- Manage return to business normal.
- Activate debrief process(es).
- Update pandemic plans as appropriate based on lessons learned.
- Update Emergency Response Plan and various business continuity plans as appropriate.
- Follow local Health authority guidelines – legislation.

Action Plan for Maintaining Essential Service/Activity

An action plan for each essential service/activity should be documented during the planning process. The SRG action plan shall include the following:

- Essential services and/or activities that must be performed to ensure the ongoing success of the organization.
- Identification of key staff members needed to perform essential services/activities and implement the action plan.
- Triggers for activating the Pandemic Planning business continuity plan.
- Identify employees that possess varied skill-sets and will be able to perform a variety of duties where needed.
- A planned strategy for communicating with staff, business partners and customers/community.

- Employee absence management procedures.
- Business reporting requirements.
- An identified chain of command for decision making processes.
- Contact information for staff members.

Change History

- Updated April 26, 2018
- Updated May 1, 2020 – Per ISNetworld specifications (safety standard requirements for Yara)
- Updated May 20, 2020 – Moved Employee Absence section to new Influenza Pandemic Control and Prevention policy, updated Scope, added Guidelines statement.

2000.53 Influenza Pandemic or Outbreak Control

Effective Date:	**April 29, 2020**
Last Updated:	**April 29, 2020**
Approved By:	**Blair Ross**

Purpose

Should an influenza pandemic or local outbreak occur, SRG will work to achieve a workplace that follows all precautionary measures identified by applicable governmental bodies and public health authorities to reduce the spread of infectious diseases in the workplace.

Employee Responsibilities

All employees should ensure they understand and comply with the infection prevention policies and practices outlined within this policy and within the Communicable Disease and Illness Control Policy.

Hand Hygiene

- Wash hands frequently. Thoroughly wash hands with an alcohol-based rub or with soap and water. Wash hands for at least 20 seconds.
- Avoid touching your face (specifically your eyes, nose, and mouth) as much as possible.
- Cover your mouth when coughing, sneezing, and yawning by doing so into the bend of your arm, not your hand.
- Avoid touching surfaces people touch often.
- Instead of a handshake, give a friendly wave or elbow bump.
- Use any necessary personal protective equipment as directed.

Workspace Cleaning

Use appropriate products provided by SRG to clean and disinfect items like your desk, work surface, phones, keyboards, and electronics at least twice daily and more often if they are visibly soiled.

Social Distancing

- Keep a distance of at least two metres between you and anyone else, including your co-workers and customers whenever possible.
- Increase distance where possible between desks, tables, and workstations.
- Limit large or crowded gatherings of personnel; and, where possible, reduce or eliminate activities that require close physical proximity or contact with people, such as team meetings.
- Limit any necessary personal proximity to others that is closer than two metres to the shortest time possible.

Updates to Management

- Provide updated emergency contact information to your manager.
- Consider whom SRG should call if you require transportation home from work.
- Immediately notify management if you rely on public transport to get to work and have no means to safety get home if you start to feel ill while at work.

Self-Isolation

If you have a symptom of the infectious disease or think you might have such a symptom, do not come to work. It is critical that if you have at least one symptom as outlined by the public health authorities (i.e. fever, cough, or difficulty breathing), or even mild symptoms, you must stay home to avoid spreading illness to others.

Additional actions you should take include:

- Immediately isolating yourself to prevent any possible spread of the infectious disease;
- Contacting your local public health authority and following their advice;
- Notifying your manager or direct supervisor and
- Remaining away from work until you have been advised to return by your public health authority, normally after a minimum of 14 days.

You need to self-isolate if you:

- Have symptoms, even if mild, associated with the illness;
- Have been diagnosed with the illness;
- Are waiting for laboratory test results after being tested for the illness or
- Have been advised to self-isolate by your regional public health authority.

Self-isolating means:

- Staying home until the regional public health authority says you are no longer at risk of spreading the illness; and
- Avoiding contact with others.

If your symptoms worsen, immediately contact your healthcare provider or public health authority and follow their instructions.

Developing Symptoms at Work

If you develop even mild symptoms while at work:

- Separate yourself from others.
- Contact your manager or direct supervisor by phone or email;
- Notify your manager where you worked that day;
- Disclose any interactions with fellow staff, customers, or others; and
- Disclose any equipment you used, items you handled, or surfaces you touched.

If you drove yourself to work, immediately go home and start self-isolating. If you took public transport, your manager will contact either your emergency contact or the local public health authority or non-emergency services to ensure that you are safety returned home.

Do not return to work until your public health authority advises it is safe to do so. The quarantine period will likely last a minimum of 14 days (or as directed by the public health authority).

Employer Responsibilities

To ensure that SRG continues to provide a healthy and safe workplace, the following measures have been implemented. In addition, SRG continues to stay updated on guidelines and information provided from the World Health Organization and the government of Canada, and on measures implemented at a provincial level.

- Use the risk-informed decision-making guidelines for workplaces and businesses during the pandemic to help develop policies and procedures.
- Continue to communicate with staff and customers about the pandemic, including the measures we are taking to prevent the spread of the illness.
- Post signs asking ill clients or customers to stay away from the premises.
- Post signs encouraging good respiratory hygiene, hand hygiene, and other healthy practices.
- Where feasible, implement measures to reduce social contact, such as teleworking arrangements, flexible hours, staggering start times, encouraging the use of e-mail, and teleconferencing.

- All non-essential meetings or travel are postponed until clearance received from the government of Canada or the local health authority.
- Continually evaluate the workplace for areas where people have frequent contact with each other and shared spaces and objects to look at measures to reduce contact.
- Ensure increased cleaning of high-contact areas.
- Evaluate and implement ways that employees can practice social distancing, such as increasing distance between desks, workstations, and people in queues.
- Minimize interactions between customers and employees.
- Implement and follow increased cleaning guidelines:
    - Make hand sanitizer available at all entries, kitchens, and common areas
    - Clean and disinfect all high-traffic areas and frequently touched areas (such as door handles, fridge handles, microwaves, printers, photocopiers) twice daily.
    - Provide cleaning wipes that are at least 70% alcohol to ensure proper disinfection, or use other approved disinfectant sprays and solutions in common areas and workspaces for employees to clean workspaces.
- Open windows and doors whenever possible to ensure the space is well-ventilated.

The following personal protective equipment is available and provided based on the following situations:

- Gloves for employees who are in direct contact with an ill person or a contaminated object or environment. Hands must be washed before putting on gloves and immediately after removing gloves. While wearing gloves, employees must refrain from touching their face. Gloves should be frequently removed and disposed to limit contact transfer.
- Heavy-duty gloves will be provided to cleaning staff.
- Additional PPE as required by regional health authorities.

Work-Related Travel

- Non-essential travel may be postponed until further notice.
- Travel for essential transportation workers is permitted as necessary.
- Essential workers are not required to self-isolate for 14 days after work-related travel, but must self-monitor closely for symptoms, and self-isolate immediately if they develop even mild symptoms.

Self-Monitoring

You need to self-monitor if you have no symptoms but may have been exposed to infection in the last 14 days, are in close contact with elderly people or medically vulnerable people, or have been instructed to self-monitor by your public health authority.

Self-monitoring means to:

- Monitor yourself for 14 days for symptoms of respiratory illness, such as cough, fever, and difficulty breathing; and
- Avoid crowded places and increase your personal space from others whenever possible.

If you develop symptoms, self-isolate immediately and contact your public health authority as soon as possible.

Employee Absence Due to Pandemic Influenza

SRG recognizes that in the event of a federally, provincially or locally declared Influenza Pandemic, the current sick leave policy may not address the needs of SRG employees.

It is imperative that a staff member who has been diagnosed with Pandemic Influenza, or has been exposed to Pandemic Influenza because a member of their household has been diagnosed with Pandemic Influenza, stay at home rather than come to work and potentially infect other staff members.

Note:

- SRG may provide paid sick leave for staff members diagnosed with Pandemic Influenza.
- Additional sick leave may be provided as needed.
- Staff members that require sick leave in excess of 3 consecutive days shall be required to provide appropriate medical documentation.

Lockdown

The following guidelines apply to the use of lockdowns as a preventive measure to combat the spread of communicable disease or illnesses in the event of a pandemic or outbreak:

- The decision to initiate a lockdown of SRG's premises shall be made by the President and COO,
- Considerations for initiating a lockdown will include, but are not limited to, the nature and severity of the threat, the possible effects on SRG employees and clients, the availability of other measures to mitigate any risks, the recommendations of public health officials, and other factors specific to the circumstances.
- The length of the lockdown will be determined by the number of cases, the severity of the illness or disease, the level of communicability, the infectious period for diseases or illnesses present, and any other relevant factors.
- During a lockdown, staff will take all necessary measures to accommodate the needs of SRG clients to the greatest extent possible. This may include:
    - Rescheduling appointments or meetings;
    - Providing information on alternative services or arrangements that are not affected by the lockdown;
    - Keeping clients up to date on developments relating to the lockdown; and
    - Notifying clients when the lockdown ends.
- If a lockdown is initiated, it shall continue until such time as the threat has been reduced or eliminated so that there is no longer significant danger to SRG employees or clients.

Change History

<Summarize changes to the previous version.>

2000.58 Hazard and Risk Assessment

Effective Date:	**October 1, 2013**
Last Updated:	**April 23, 2020**
Approved By:	**Blair Ross**

Purpose

SRG realizes that needless accidents and injuries or damages can occur if there is no formal program in place to identify and assess hazards and safety risks in the workplace.

Scope

This policy applies to all SRG employees.

Policy

Prior to assigning security officers to a site, our five step Job Hazard Analysis / Risk Assessment shall be performed. All potential hazards will be identified and classified according to risk.

A Job Hazard Analysis / Risk Assessment should be performed on a regular basis and when there a change to normal processes.

SRG requires all security officers assigned to sites that have potential hazards and safety risks to undergo site-specific training to identify the types of encroachment activities that could endanger the worksite. All on-site employees are actively involved in the hazard identification process. Employees are to be familiarized with the types of hazards that may be observed at specific worksites so proper judgement can be used to escalate the matter in a dangerous situation.

Serious incidents must be reported to OH&S/WCB immediately.

Procedure

The goal of Job Hazard Analysis / Risk Assessment is to eliminate a hazard or reduce the level of its risk to as low as reasonably achievable by implementing control measures, as necessary. The following five steps are used to assess risk:

1. Analyze Risk
2. Classify and Rank Risk
3. Control Risk
4. Control Implementation
5. Review and Improve

Control Measures

First, attempt to eliminate the hazard. If elimination is not practicable, use engineering controls. If engineering controls are not practicable, implement administrative controls. If the hazard cannot be adequately controlled using engineering and/or administrative controls, employees must use Personal Protective Equipment. A combination of engineering controls, administrative controls, and Personal Protective Equipment is usually best.

Immediately upon identification of a potential hazard and/or safety risk, contact the site supervisor, the Field Manager, the 24-hour SOC or the Manager of Operations immediately. Always consider your own personal safety **AT ALL TIMES**.

Should you consider that a situation is beyond your training or abilities, call for assistance. Stand back, observe and take notes, rather than risk your own safety and become a casualty.

All identified hazards must be reviewed by all affected employees.

Additional Information

Refer to the SRG Safety Policies and Procedures document for complete detail.

Change History

April 23, 2020 – Added reference to the SRG Safety Policies and Procedures document.

2000.60 Human Rights, Anti-Harassment, Anti-Discrimination

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

The Canadian Human Rights code protects the rights of Canadians. Under the code, SRG, as an employer, has the legal responsibility to ensure the right of every employee to work in an environment free of harassment and discrimination. SRG is committed to providing a harassment and discrimination free workplace. In order to achieve this goal, both SRG and each employee must assume certain responsibilities.

Scope

This policy applies to all employees of SRG regardless of position, employment status or title.

Legislative Context

Both the Canadian Human Rights Act and the Canada Labour Code protect employees from harassment related to work. Provincial human rights laws also prohibit harassment. The Criminal Code protects people from physical or sexual assault

Policy

- SRG recognizes every person has the right to fair treatment with respect to employment without discrimination because of race, ancestry, place of origin, colour ethnic origin, citizenship, creed, religion, sex, sexual orientation, age, family status or disability.
- SRG will provide education to enable employees to become aware of what constitutes harassment and discrimination and what resources are available to resolve complaints.
- All SRG employees have the responsibility and are expected to respect the rights, dignity and self-esteem of others.
- Any employee found to be engaged in or who has engaged in conduct that is contrary to this policy will be subject to appropriate disciplinary response up to and including termination of employment.

All SRG employees have the responsibility and are expected to respect the rights, dignity and self- esteem of others.

SRG shall investigate all complaints of harassment or discrimination. All complaints are taken seriously. All complaints and investigations must be documented.

Procedure

Processing and Mediation of Harassment and Discrimination Complaints

Step 1 – Informal Procedure

Where possible, the employee is encouraged to resolve the matter directly with the individual(s) involved.

Step 2 – Complaints

If the employee(s) feels that resolving the issue is unsuccessful or inappropriate, the employee must file a complaint with their Supervisor or Manager, within twenty-five (25) working days from the end of the informal procedure.

The supervisor or manager has an obligation to advise the Regional Manager of any complaint made under this step. The supervisor or manager in consultation with the Regional Manager will investigate and implement appropriate action, summarizing the finding and action in a report.

Note: If your manager or supervisor is involved in the problem, report the problem to the Regional Manager. If the Regional Manager or higher is involved, report to the President and COO.

Step 3 – Final Recourse

Any employee who feels that the report and action taken does not address his or her concerns may file a complaint with the Manitoba Human Rights Commission.

Change History

<Summarize changes to the previous version.>

2000.65 Incident Reporting & Investigation

Effective Date:	**October 1, 2013**
Last Updated:	**October 1, 2013**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that if incidents go unreported, proper corrective actions may not be taken which may perpetuate the problems in the future.

Scope

This policy applies to all SRG employees.

Policy

All incidents are to be reported immediately after they occur. All incidents are investigated and followed up with the proper corrective action or disciplinary action. When SRG becomes aware of an incident, SRG will appoint a qualified person to carry out an investigation. All work-related injuries and illnesses are to be documented.

Procedure

If an employee is involved in a work-related incident or is aware of a condition that may cause one, the employee must report the incident to SRG immediately to a site supervisor, the Field Manager, the 24-hour SOC or the Manager of Operations. Incidents include break and enters, injuries, medical emergencies, illnesses, fire/police/ambulance, bomb threats, property damage, etc.

All reports should be in writing and signed by the employee(s) involved and reasonable evidence regarding the incident shall be available. All incidents will be investigated by individuals deemed qualified and competent by SRG. The incident report must include a description of the incident (who, what, where, why, when and how), any evidence collected during the investigation, an explanation of the causes and/or contributing factors of the incident, and the recommended corrective actions. After receiving the result of the documented investigation, it will be determined whether corrective action should be taken regarding the incident, employee or situation in general. The corrective action should reduce the opportunity of the incident recurring.

Action in this regard may include a direction regarding counselling or other remedial action, a reprimand, a suspension or termination of employment.

SRG will take action where it considers it appropriate to do so whether the circumstances arise by virtue of an incident report from a member of the public or supplier or, whether SRG otherwise determines that such action is necessary.

Team members performing investigation work are provided training on investigation techniques.

Change History

<Summarize changes to the previous version.>

2000.70 Injury on the Job

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

Safe work practices are of prime importance to SRG. Our policy objective is to provide and maintain a safe and healthy working environment.

Scope

This policy applies to all employees of SRG and any sub-contractor of SRG.

Policy

In the event of an accident/incident involving a company employee, the supervisor should be advised as soon as possible. The employee can call the local office management as well.

Note: Any employee injured as a result of a work-related accident/incident must complete and submit a Workers' Compensation "Notice of Injury" Report within 48 hours of the event to their supervisor.

Procedure

All employees of SRG share responsibility for safety and accident prevention. This responsibility can be met by ensuring that employees are properly trained for the job and to ensure that property and equipment are maintained within acceptable standards.

Employees should report all unsafe equipment or conditions immediately to their supervisor.

If you have any concerns or questions relating to safety or health issues, please contact your supervisor or a member of the Workplace Safety and Health committee.

Change History

<Summarize changes to the previous version.>

2000.80 Leave of Absence

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that employees may require time away from work for personal or other justifiable reasons. This policy is established to create a work environment that allows employees the flexibility to better manage their work and personal lives while meeting operational requirements.

Scope

This policy applies to all SRG personnel.

Policy

SRG shall grant paid or unpaid leave of absences to employees in accordance with applicable legislation and employment contracts. SRG may grant a leave of absence to eligible employees for periods beyond legislative requirements or employment contracts subject to exigencies of service and other established criteria. A minimum of thirty (30) days' notice is required to apply for a leave of absence.

Procedure

Employees requesting unpaid leave in excess of ten (10) working days must contact their supervisor to discuss the effects on benefits and coverage.

Change History

<Summarize changes to the previous version.>

2000.85 Long Term Disability

Effective Date:	**October 1, 2013**
Last Updated:	**October 1, 2013**
Approved By:	**Blair Ross**

Purpose

SRG employees with Long-term Disability (LTD) are subject to this policy.

Scope

SRG Employees with Long-term Disability coverage.

Policy

Long-Term Disability benefits can be received to a maximum of 12 months from the time the benefits commence. To receive the benefit the SRG employee must pay SRG the LTD premium uninterrupted. In order to qualify for payout of the LTD benefit the SRG employee must provide written documentation from a doctor.

Procedure

SRG employees must coordinate through their respective manager in the event an LTD claim will be made.

Change History

<Summarize changes to the previous version.>

2000.112 Manual Material Handling

Effective Date:	**October 1, 2013**
Last Updated:	**May 19, 2020**
Approved By:	**Blair Ross**

Purpose

Manual material handling refers to any tasks involving lifting, carrying, pushing or pulling objects. SRG realizes that muscle overuse or overexertion injuries can occur when the task is performed without pre- conditioning the muscles and joints or when the demands exceed the body's physical capabilities. Muscle overuse and overexertion injuries can range from swelling and soreness to torn muscle, tendons or ligaments. Mechanized equipment should be used for material handling, whenever practicable.

Scope

This policy applies to all SRG employees.

Policy

SRG requires that Security Officers assigned to sites that require lifting understand there is no single, safe "limit" with regards to lifting items

SRG requires that Security Officers assigned to sites that require lifting are trained on use safe lifting techniques as this is important for reducing the risk of injury when lifting (or lowering) items.

Procedure

Lifting/Lowering

SRG requires that all SRG employees understand there is no single, safe "limit" with regards to lifting items. The risk of injury from lifting (or lowering) depends on a number of factors that need to be considered including:

- Size, shape and weight of the package
- Male vs. Female population
- Hand placement (i.e. how far away from your body are your hands?)
- Position of the load (below knees, waist height, above shoulders)
- Do you twist your body during the lift?
- Shape and weight of the load
- Number of lifts performed (frequency)

General Safe Lifting Technique

SRG requires all personnel be trained on use safe lifting techniques as this is important for reducing the risk of injury when lifting (or lowering) items. Remember, let your legs do the work, not your back. Also, be sure to avoid awkward postures such as reaching too far and twisting your back. General lifting and lowering technique involve:

- Sizing up the load
- Standing close to load, with feet apart (shoulder width)
- Squatting down – bend at hips and knees
- Arching lower back inward and keep back straight
- Keeping the load close to body
- Turning your feet when changing direction
- Placing load down - squat (bend at knees, keep lower back arched inward)

Pushing/Pulling and Carrying

Using safe techniques is also important for reducing the risk of injury when pushing, pulling or carrying items. Remember, it's generally easier, and safer, to push than to pull. Pushing uses your body weight to move the load and this position allows you to see where you're headed. Also, avoid carrying heavy objects too far. Consider using a cart, dolly or other wheeled or mechanical device instead. The forces required, and the risk of injury, to push, pull or carry a load depends on a number of factors that need to be considered including:

- Male vs. Female
- Hand placement
- Distance involved
- Number of lifts performed (frequency)
- Floor surface
- Size, shape and weight of the package
- Condition of floor, wheels

Change History

May 19, 2020 – Broadened scope to include all SRG employees.

2000.113 Fatigue Management

Effective Date:	**July 1, 2019**
Last Updated:	**May 19, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that fatigue may present as a factor that adversely affects a worker's ability to perform mental and physical tasks. Due to the nature of guard work, our employees may suffer from fatigue due to long drives to and from remote work sites and/or sleep deficit caused by long hours and on-call duties.

All personnel must be able to recognize and respond to the signs and symptoms that might impair the worker's performance due to fatigue. Training will be provided to recognize and respond to fatigue issues in the field.
It is the responsibility of the (Appropriate Authority) to make corresponding changes to work requirements if signs of impairment due to fatigue are evident. All concerns should be communicated to management and corresponding changes should be documented for review and follow-up.

The development, implementation and continual monitoring of our Fatigue Management Policy is intended to ensure that Security Resource Group provides a safe and healthy work environment for all employees, and the public at large.

The purpose of the Fatigue Management Policy is to ensure that management, supervisory personnel and employees understand what fatigue is, how extended hours of work or consecutive days of work can affect fatigue and the proper proactive methods of effectively dealing with worker fatigue.

Scope

This policy applies to all SRG employees operating vehicles, working with equipment, or working in any area where hazards exist

Guidelines

Definition

Fatigue is defined as a state of being tired. It can be caused by long hours of work, long hours of physical or mental activity, inadequate rest, excessive stress, and combinations of these factors. The signs, symptoms and effects fatigue have on workers varies from one person to the next; however, fatigue may affect the individual worker's ability to perform mental and physical tasks.

Signs, Symptoms, Factors and Performance Impairments

Some of the possible physical signs and symptoms are as follows:

- Tiredness
- Sleepiness
- Irritability
- Depression
- Giddiness
- Loss of appetite
- Digestive problems
- An increased susceptibility to illness

Potential Impairments to Performance

- Slowed reactions - physical reaction speed and speed of thought
- Failure to respond - to stimuli, changes in the surroundings, information provided
- Incorrect actions - either physical or mental
- Flawed logic and judgment and an increase in memory errors, including forgetfulness
- Decreased vigilance
- Reduced motivation
- Increased tendency for risk-taking

Factors Which May Have an Influence on Fatigue

- Time of day
- Temperature
- Working alone
- Repetitive functions
- Physical inactivity
- Length and frequency of breaks
- Availability of food and water
- Duration of the extended hours/consecutive days
- Long periods of driving to and from remote work sites
- Days off
- Type of work
- Job stress
- Home stress
- Non-effective use of personal time
-

Responsibilities

Management

- Ensure the Fatigue Management Policy is implemented throughout the company
- Provide the necessary information about fatigue
- Provide instruction and training
- Communicate employer expectations
- Monitor the effects of extended work hours
- Support employees who are experiencing concerns with fatigue
- Assist and advise Supervisors
- Investigate any problems and/or concerns
- Inspect the workplace and review policy with employees
- Review the Fatigue Management Policy when necessary

Supervisors

- Ensure all employees under your direction understand the policy
- Conduct safety meetings discussing fatigue and the policy
- Promote the Fatigue Management Policy
- Ensure tasks are performed in safe and healthy manner
- Ensure employees are paired up to create a buddy system when required to drive for long periods of time
- Be aware of the possible risks associated with extended hours and/or consecutive days of work
- Give workers as much notice as possible if extended hours are anticipated
- Observe and record how individuals respond to extended hours
- Recognize symptoms of fatigue
- Get feedback from individual crewmembers and the crew as a whole

- Take prompt action if a risk develops
- Relay information to and from management and employees
- Report any problems, concerns and/or issues

Employees

- Actively participate in Fatigue Management education training
- Recognize symptoms of fatigue
- Promptly report any fatigue related concerns
- Share driving responsibilities with another worker when driving for long periods of time
- Report any individual medical or personal situations, which may have an effect on fatigue
- Ensure that they provide themselves with proper rest during time off
- Identify personal stress and seek assistance if required

Preventive Methods for Dealing with Fatigue

- Inform all workers of the Fatigue Management Policy
- Ensure that workers are always provided with a minimum of eight hours off between shifts
- Ensure that workers do not work for more than 24 days consecutively
- Ensure that employees understand that the effect of fatigue can be compounded by the abuse of alcohol, poor diet, lack of exercise, personal problems, depression, lack of sleep or sickness
- Utilize a buddy system when employees are required to drive for long periods of time to ensure driving responsibilities are shared
- Ensure that fatigue is accounted for in project and daily planning
- Minimize extended hours of work when possible
- Schedule rest days
- Assess and control hazards and risks
- Provide an honest, open and healthy work environment
- Provide information and assistance
- Recognize individual and crew fatigue
- Give as much advance notice of extended hours as possible
- Define whether the work is urgent or not
- Ensure that employees have access to food and water
- Take short and frequent breaks
- Provide employees with options such as transfers, job sharing, etc.
- Solicit short-term help to minimize the need for extended hours
- Have employees rotate and perform various functions of short duration during extended hours
- Perform complex tasks earlier in the shift, if possible
- Account for employees returning from sickness, absences and/or modified work
- In conjunction with employees, identify health problems which may affect an employee's ability to work extended hours (i.e., diabetes)
- Be flexible and supportive when dealing with an employee with problems at home
- Consider travel time to and from work

Reporting Procedures

- Report any unsafe acts, incidents, and near misses
- Inform Management if a crew or an individual has a concern working extended hours
- Develop a process to identify and report when a crew or an individual is working extended hours and/or excessive consecutive days

Monitoring Methods

- Management/supervisors to monitor crew's hours of work

- Management/supervisors to determine the need for extended hours
- Management/supervisors are to monitor crews when working extended hours for fatigue related concerns
- Management/supervisors are to address crewmember concerns regarding working extended hours
- Management shall monitor supervisor/employee relationships
- Ensure everyone has been trained in the Fatigue Management Policy

Program Review Processes

- Periodically review Fatigue Management Policy and procedures
- Compare ratio of crews working extended hours to those not working extended hours
- Determine and review the reasons and factors for working extended hours
- Perform and review employee/Supervisor extended hours of work survey
- Review the effectiveness of the Fatigue Management training program
- Review the factors affecting the need for extended hours
- Discuss possible alternatives to extended hours of work.

Change History

May 19, 2020 – Updated Guidelines to reflect current practices.

2000.120 Safety Hazards

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

Due to the nature of the work that personnel may be asked to do, safety concerns and issues may be brought to our attention. While on patrol or responding to a problem, personnel need to be aware of and think about all potential safety hazards that may need immediate attention. Our policy objective is to provide and maintain a safe and healthy working environment by spotting the potential hazards.

Scope

This policy applies to all employees of SRG.

Policy

Prevention of needless accidents and injuries or damages is very important. Personnel should not ignore the potential safety problems. If in doubt, contact your supervisor, the Field Manager, the 24-hour SOC or the Manager of Operations immediately.

Always consider your own personal safety **AT ALL TIMES**.

Should you consider that a situation is beyond your training or abilities, call for assistance. Stand back, observe and take notes, rather than risk your own safety and become a casualty.

Procedure

All employees of SRG share responsibility for safety and accident prevention. This responsibility can be met by ensuring that employees are properly trained for the job and to ensure that property and equipment are maintained within acceptable standards.

Employees should report all unsafe equipment or conditions immediately to their supervisor.
When dealing with the removal of persons from a site please ensure that proper safety equipment (rubber gloves), and procedures are followed.

If you have any concerns or questions relating to safety or health issues, please contact your supervisor or a member of the Workplace Safety and Health committee.

Types of Hazards

- Wet Floors
- Obstructed Fire Exits
- Broken Glass
- Chemical/fuel spills
- Tripping Hazards
- Sharp Objects
- Gas Leaks
- Poorly secured objects
- Ice Patches
- Water Leaks
- Dangerous Activities

Many other hazards can occur, too many to mention. Please follow the policy as listed above.

Additional Information

Associated Documents:

- Security online training Lestac (Bloodborne Pathogens in Chapter #)
- Guidelines for Thermal Stress (Workplace Health and Safety)

Change History

<Summarize changes to the previous version.>

2000.150 Smoking

Effective Date:	**June 29, 2012**
Last Updated:	**April 24, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that some employees smoke however smoking/vaping while on duty is not permitted.

Scope

This policy applies to all employees/contractors.

Legislative Context

Smoking is not permitted in any public areas as defined in the Tobacco Control Act.

Policy

Smoking is not allowed by any SRG employee while they are on duty. This includes any kind of cigarette including electronic cigarettes (Vaporizer or inhalant-type devices)

Procedure

SRG employees are only allowed to smoke when they are on their authorized coffee and/or lunch break and only in designated locations.

Failure to follow the smoking policy will result in disciplinary actions which could include termination.

Change History

April 24, 2020 – added electronic cigarettes (Vaporizer or inhalant-type devices).

2000.180 Temporary Contracts

Effective Date:	**June 29, 2012**
Last Updated:	**April 23, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that temporary clients will call and inquire about our services.

Scope

This policy applies to all locations.

Policy

When a client calls and wants to hire SRG for Security Services and the client is not recognized in SRG's client database, where possible a 50% cash deposit on the estimated invoice total must be obtained two (2) weeks prior to any work commencing.

Procedure

Complete a Service Detail Report (SDR) form. Ensure operations and finance receive copies of the contract. Create and fill schedule in Intime. Pricing is based on prescribed rates or others as approved based on Policy Number 4000.01.

Change History

April 23, 2020 – Add information about utilizing the SDR.

2000.195 Dress Code – Management & Administrative Personnel

Effective Date:	**October 1, 2013**
Last Updated:	**April 23, 2020**
Approved By:	**Blair Ross**

Purpose

SRG encourages its employees to dress comfortably. However, it is critical that employees of SRG maintain a professional appearance while in the workplace, or while attending company-sanctioned events offsite. As such, appropriate attire should be worn at all times, in keeping with recognized standards, in order to project a positive image.

Scope

This policy applies to SRG Management and Administrative Personnel

Policy

Personnel shall dress in a manner commensurate with the designated responsibilities of their job roles or their audience.

Procedure

Employees are expected to wear semi-formal business attire on a daily basis. This can include suits, dress slacks, sports jackets, dress or sport shirt, dresses, skirts etc. Tie is not mandatory but is recommended depending on the audience.

For employees who interact with clients and customers, even if only on an occasional basis or via the telephone, these workers must dress appropriate to the audience.

Tattoos and Body Piercing

Employees with tattoos must cover them at all times while at work or company-sanctioned events. Body piercings, except for women's earrings, must be removed prior to coming in to work or attending company-sanctioned events.

Additional Information

Casual Fridays

Every Friday, SRG Management and Administrative personnel may dress down unless they are acting in a representative capacity that day and are required to wear Business Formal attire. For employees who may get called to see a client at a moment's notice it is recommended they keep a change of business clothes available if wearing Casual Friday attire.

On Casual Friday, staff may wear jeans (new condition), khakis, casual skirts, shirts with collars, sweaters and casual footwear.

Change History

April 23, 2020 – amend Casual Fridays applicability.

2000.200 Vacation

Effective Date:	**June 29, 2012**
Last Updated:	**May 19, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that employees are entitled to receive annual vacation leave

Scope

This policy applies to all staff.

Legislative Context

This policy operates under the broad framework of the *Labour Standards Act* of the respective province and/or applicable Collective Agreements.

Policy

All personnel must provide SRG with a minimum of thirty days (30) notice for all vacation requests.

Procedure

Employees of SRG, after successful completion of their probation period, shall receive annual vacation leave in accordance with Provincial Legislation and/or applicable Collective Agreements.

One (1) year of employment is required to be eligible to request Vacation time off.

All employees must provide a minimum of thirty days (30) notice for all vacation requests. All requests are on a first come first serve basis and must be submitted to their immediate supervisor.

Vacation pay requests must be submitted in writing on an SRG Request for Time Off form and will be paid on the pay cheque following the request. Vacation pay will not be paid out on a separate cheque.

All vacation leave requests are dependent on operational requirements.

Change History

April 24, 2020 – Added Collective Agreements as a guiding policy if applicable.
May 19, 2020 – Added Request for Time Off form to Procedures.

2000.215 Workplace Cleanliness

Effective Date:	**April 29, 2020**
Last Updated:	**April 29, 2020**
Approved By:	**Blair Ross**

Purpose

SRG has adopted this policy to ensure the ongoing health and safety of our employees, and to provide a safe and healthy working environment. SRG will ensure that our work environment is maintained in a clean and organized fashion as to minimize hazards to our employees.

Scope

This policy applies to all SRG employees (and contractors working on behalf of SRG) while they are engaged in company business, working on company premises or worksites, and operating company vehicles and equipment.

Guidelines

SRG work spaces shall be maintained in a clean and organized manner in order to ensure employees are working in a safe and healthy work environment. Work surfaces must be disinfected on a regular basis to eliminate dirt and the spread of germs. The following steps are to be followed:

- Clean visibly soiled surfaces before disinfecting
- Wear appropriate gloves when in contact with chemical solutions, and where specified by the manufacturer
- Prepare solutions for cleaning and disinfection daily. It is important that proper strengths of disinfectant solutions are used
- Follow the manufacturer's instructions for the safe and proper application of specific cleaning and disinfecting products
- Ensure all WHMIS protocols including any information found on the SDS for the cleaning solution being used are followed

Ensure daily disinfecting of surfaces and objects that are touched often. Items that require daily disinfecting include, but are not limited to:

- Desks
- Countertops
- Doorknobs
- Bathrooms
- Computer keyboards
- Faucet handles
- Phones
- Toys

Include any other items that required to disinfected on a daily basis

Change History

<Summarize changes to the previous version.>

2000.220 Workplace Safety & Health

Effective Date:	**June 29, 2012**
Last Updated:	**April 24, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes the necessity to maintain a healthy workplace and environment for the employees. Employees' safety is our first priority.

Scope

This policy applies to all employees of SRG.

Legislative Context

The purpose of Part II of the *Canada Labour Code* is to prevent work-related accidents and diseases in companies and organizations under federal jurisdiction. Each Province has legislated requirements that SRG employees must adhere to. At the same time, however, both employers and employees have key roles to play in achieving this goal.

Policy

SRG management and employees will comply with the Occupational Health & Safety (OHS) Act and its regulations. SRG will consult and co-operate with any OHS committee or representative at the place of employment for the purpose of resolving concerns on matters of health, safety and welfare at work.

Procedure

All employees must report and unsafe working condition to their Site Supervisor or SRG management immediately. The unsafe working condition or area must be investigated by the Site Supervisor or SRG management upon notification. If the unsafe condition requires the attention of the client, SRG management will speak with the client and ensure the matter is taken care of.

No employee will be required to work in any unsafe working environment and will be directed to avoid working in that specific area until it has been deemed safe. A detailed report must be filled out by SRG management and a copy of the report must be sent to the SRG Director of Protective Services. A copy of the report will be placed on the clients file.

Hazard Identification

SRG recognizes that site Hazard Identification Inspections are to be performed at sites and are normally completed on a monthly basis:

Formal Workplace Inspections

Every workplace inspection must examine who, what, where, when, why and how. Inspect the entire work area each time. Include areas where no work is done regularly, such as parking lots, rest areas, office storage areas and locker rooms. Pay particular attention to items most likely to develop unsafe or unhealthy conditions because of stress, wear, impact, vibration, heat, corrosion, chemical reactions or misuse.

Look at all workplace elements relevant to your working area - the environment, the equipment and the process. The environment includes such hazards as noise, vibration, lighting, temperature, and ventilation. Equipment

includes materials, tools and apparatus for producing a product or a service. The process involves how an employee interacts with the other elements in a series of tasks or procedures.

Prior to beginning a workplace inspection - know your workplace. To help ensure a systematic approach to the inspection, obtain an up-to-date floor plan of the workplace. Looking at the floor plan, determine what hazards are applicable to the work area to ensure that all areas of the workplace are inspected.

Who Should Formally Inspect the Workplace?

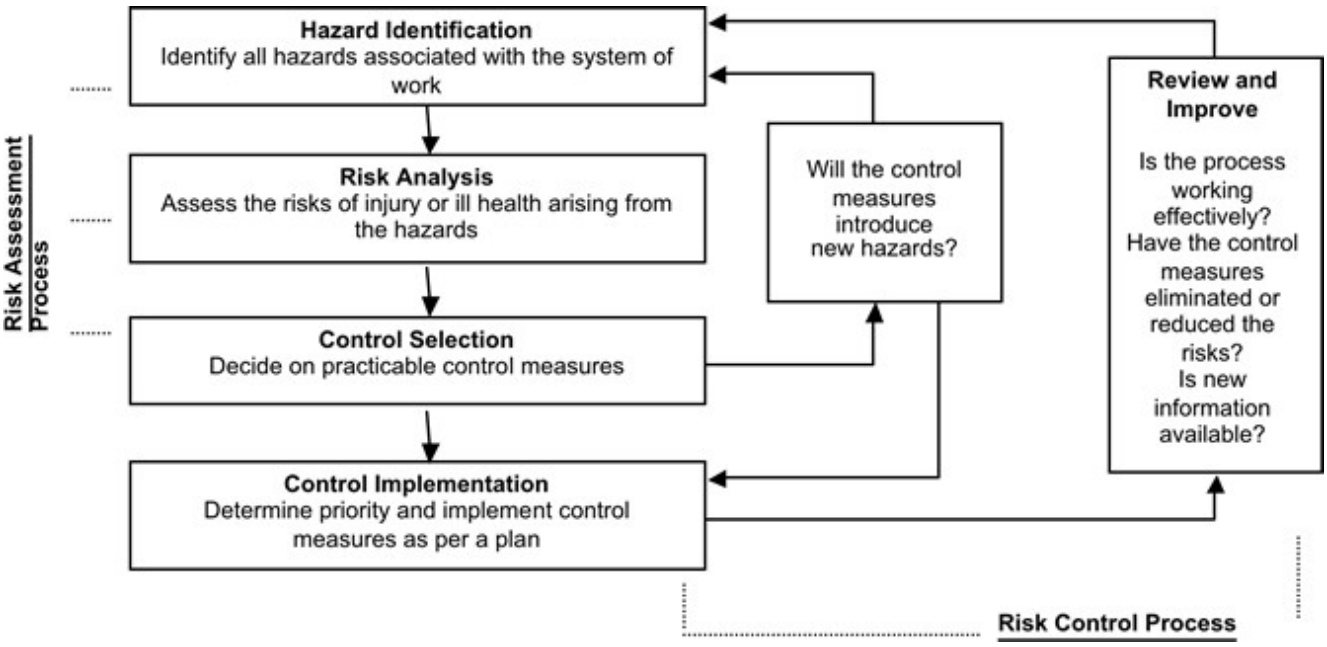
The employer is responsible to ensure that employees are made aware of any hazard in their workplace. Supervisors are responsible to advise employees of any hazards or potential hazards that exist in the workplace. Employees are responsible to report any hazards or potential hazards to their supervisor.

Risk Assessment

Every hazard that is identified can be assessed for risk. However, hazards that continue to arise, despite regular mitigation, and hazards with significant budgetary implications are those hazards commonly assessed for risk. The goal of the risk assessment process is to remove a hazard or reduce the level of its risk to as low as reasonably achievable by implementing control measures, as necessary. The following four steps are used to assess risk:

1. Analysing Risk
2. Controlling Risk
3. Control Implementation
4. Review and Improve

Health & Safety Risk Management Cycle



Structure and Responsibilities

Security Supervisors

Supervisors have the following responsibilities:

- Understanding their responsibilities and duties under the Occupational Health and Safety Act

- Informing employees of their rights, responsibilities and duties under the OHSA and the department's HSMS, including their right to refuse unsafe work; and
- Ensuring that workplace incidents and injuries are reported and investigated promptly, and that corrective action is taken.

Supervisors are also responsible under Occupational Health and Safety Act to ensure that employees under their direction and control:

- Are properly instructed, and their work is performed without undue risk.
- Use or wear the equipment, protective devices, or clothing required under the OHSA or by the nature of the work.
- Are advised of the existence of any potential or actual danger to their health or safety of which the supervisor is aware.
- Are provided with written instructions as to the measures and procedures to be taken for the protection of the employee.

Employees

Employees have the following responsibilities:

- Knowing and acting upon their duties and rights under the Occupational Health and Safety Act.
- Following their supervisor's and department's instructions on health and safety.

Additional Information

Associated Document: SRG Safety Policy and Procedures Manual

Change History

April 24, 2020 – denote each Province has legislation that SRG employees must follow; refer to SRG Safety Policy and Procedures Manual for current details

2000.225 Workplace Violence

Effective Date:	**October 1, 2013**
Last Updated:	**May 19, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that employees could be exposed to and harmed by workplace violence.

Scope

This policy applies to all SRG employees.

Legislative Context

Each Province has legislation that SRG employees must follow.

Policy

SRG is committed to protecting all SRG employees and shall take reasonable precautions, including training, to prevent workplace violence.

SRG shall assess, and reassess as necessary, the risks of workplace violence that may arise from the nature of the workplace, the type of work or the conditions of work.

Anyone who engages in workplace violence shall be subject to complaint procedures, investigation, remedies, sanctions and discipline up to and including termination.

Procedure

Incidents of workplace violence must be reported and investigated. When SRG becomes aware of workplace violence or alleged workplace violence, SRG will investigate the matter.

All reports should be in writing and signed by the employee(s) involved and reasonable evidence regarding the incident shall be available. All incidents will be investigated by individuals deemed qualified and competent by SRG. The investigation report must include a description of the incident, any evidence collected during the investigation, an explanation of the causes and/or contributing factors of the incident, and the recommended corrective actions. After receiving the result of the investigation, it will be determined whether corrective action should be taken regarding the incident, employee or situation in general. The corrective action should prevent the recurrence of the incident.

Action in this regard may include a direction regarding counselling or other remedial action, a reprimand, a suspension or termination of employment.

Change History

April 24, 2020 – Note that each province has its own legislation that SRG employees must follow.
May 19, 2020 – Broadened Scope to include all employees.

FINANCIAL AUTHORITY

3000.10 Financial / Signing Authority

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

SRG recognizes solid financial control with signing authority controls contribute to the success and financial health of an organization.

Scope

This policy applies to all staff.

Policy

Signing Authority for SRG and its subsidiaries rests with the President & COO and/or the Chair & CEO or in some instances an authorized designate may suffice. An authorized designate is a person authorized by the President & COO and/or the Chair & CEO to sign on behalf of the company for a specific matter.

Cheques – signed by both the President & COO and the Chair & CEO.

Leases – approved and signed by the President & COO or the Chair & CEO or an authorized designate.

Contracts – rates approved and signed by the President & COO or the Chair & CEO or an authorized designate.

Employee Wages/Benefits – All wages, salaries and benefits are approved by the President & COO or the Chair & CEO.

Bad Debt Write-offs – approved by the President & COO or the Chair & CEO.

Expense Claims – first approval by applicable manager and final approval by the President & COO or the Chair & CEO.

Payroll Submissions – are to be made on time in accordance to applicable legislation. First approval by applicable manager and final approval by the President & COO or the Chair & CEO.

Payroll Corrections – first approval by applicable manager and final approval by the President & COO or the Chair & CEO or an authorized designate.

Collective Bargaining Agreements – approved and signed by the President & COO or the Chair & CEO or an authorized designate.

Division/Region Payables – pre-approved payables are to be initialled to confirm accuracy by the respective Manager.

Budgets – are approved by the Board of Directors and form the basis by which the company is managed from a financial and growth point of view.

Other – applies to any other finance or signing issue not contemplated above. Approval and signed by the President & COO or the Chair & CEO or an authorized designate.

Procedure

The following are guidelines to follow:

Cheques – are prepared by finance following required approval and are signed by both the President & COO and the Chair & CEO

Leases – are pre-approved by the President & COO or the Chair & CEO and then signed by the President & COO or the Chair & CEO or an authorized designate

Contracts – billing rates are pre-approved by the President & COO or the Chair & CEO and signed by the President & COO or the Chair & CEO or an authorized designate

Employee Wages/Benefits – All management salaries and benefits are approved by the President & COO or the Chair & CEO. Other Employees or Consultants are to be paid in accordance to prescribed pay rates determined by the President & COO or the Chair & CEO. Any deviation must be approved by the President & COO or the Chair & CEO.

Bad Debt Write-offs – are approved by the President & COO or the Chair & CEO and submitted to finance. In the instance a client will not pay an email to finance explaining situation is required.

Expense Claims – are submitted on the prescribed Expense Claim form at the end of each calendar month, approved and signed by the President & COO or the Chair & CEO and submitted to finance for payment

Payroll Submission – Payroll is reviewed by Finance and approved by the President & COO or the Chair & CEO, or a designate, prior to submission

Payroll Corrections – are submitted on the prescribed Payroll Correction Form and approved by the President & COO or the Chair & CEO or an authorized designate

Collective Bargaining Agreements - approved and signed by the President & COO or the Chair & CEO or an authorized designate

Budgets – are approved by the Board of Directors and form the basis by which the company is managed from a financial and growth point of view. Budget “owners” must ensure “day to day” expenses do not exceed the Budget based on the overall budget. Any deviation must be approved by the President & COO or the Chair & CEO. Large purchase items while contemplated in the budget must be approved by the President & COO or the Chair & CEO. These include but are not limited to Vehicles, Computer equipment, Uniforms, office furniture.

Other – applies to any other signing issue not contemplated above. Approval and signed by the President & COO or the Chair & CEO or an authorized designate

Change History

<Summarize changes to the previous version.>

3000.20 Payroll Administration

Effective Date:	**June 29, 2012**
Last Updated:	**May 13, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that payroll functions, completed accurately and timely, will strengthen the overall financial health of the organization and will help maintain positive business relationships with employees. The intent of this policy is to communicate SRG's payroll processes and procedures.

Guidelines

- SRG utilizes consistent and comprehensive payroll processes and procedures in order to ensure that its employees are paid appropriately and on time.
- SRG employees in the Protective Services Division will be paid on a bi-weekly basis with remuneration to be directly deposited into the employee's bank account (or via cheque if direct deposit unavailable) every second Friday.
- SRG employees in Management, Administration, and Cyber Security Division will be paid on a twice-monthly basis with renumeration to be directly deposited into the employee's bank account (or via cheque if direct deposit unavailable) on or before the 15th of each month and on or before the final day of each month.

Legal Compliance

SRG shall ensure its payroll processes and procedures comply with all relevant legislation and adhere to all reporting and tax withholding requirements.

Furthermore, SRG shall ensure all payroll and compensation information obtained is stored and maintained in a secure area. Such information shall only by shared for payroll, administrative and legal purposes.

Workplace Responsibilities

Employees

- Upon hire, employees must immediately complete and submit required federal and provincial income tax forms and all other associated payroll paperwork. Federal and provincial tax forms will be utilized by the organization in order to calculate statutory deductions as required by law such as CPP, IE and Income Tax.
- Upon hire employees must submit to their manager their current banking information in order to facilitate the direct deposit process.
- Must promptly inform management of any changes to banking information during employment.
- Accurately document and report all hours worked.
- Immediately inform management of any identified discrepancies in payment.
- Comply with all departmental procedures for the collection of information pertaining to SRG payroll processes.

Management

- Ensure all new hire and payroll information is collected and submitted to the payroll administrator in a timely and accurate manner.
- Ensure all collected and retained employee information pertaining to remuneration remains confidential and is only disclosed to authorized personnel.
- Accurately maintain record of all sick, vacation, and all other time away from work taken by direct reports.
- Provide assistance or forward inquires to the payroll coordinator pertaining to remuneration concerns.

Payroll/Finance Department

- Update and maintain the company's payroll information system with new employee information, terminations, leaves, updated banking information etc.
- Process payroll information in a timely and accurate manner to ensure staff are paid accurately and on schedule.
- Accurately calculate all required statutory deductions.
- Provide accurate and timely report to relevant departments and government agencies as required.
- Accurately process TD1s and all other relevant documentation.
- Respond to inquiries from employees, management, government agencies and all other relevant parties.
- Maintain confidentiality concerning employee payroll information and remuneration.

SRG Security Resource Group Inc.

- Comply with all provincial, federal and legal payroll requirements, duties and responsibilities pertaining to taxation and reporting.
- Create, maintain and update as required consistent and comprehensive payroll processes and procedures.

Procedures

All employees to whom this policy applies must follow the invoicing procedures set forth below. Deviating from such procedures is not acceptable and may warrant disciplinary action.

1. Protective Services Division Payroll

InTime Setup and Reporting

- Each operating group is to be separated into branches in InTime with a complete list of Customers. Each Customer is to be assigned a location(s), which organizes customers who have multiple locations.
- As per policy InTime must be updated on a daily basis. Reports are generated for different periods, and it is important that InTime always reflects the most up to date information.
- The report used for payroll is the Payroll Detail by Employee. This report must be submitted to the payroll administrator, or verified as ready for processing, by 9:00am Saskatchewan Time on the Monday prior to payroll submission. *Note: Payroll schedule/submission dates may be advanced during pay periods in which a statutory holiday occurs.*

Payroll Adjustments and Forms

- Each branch must have one person designated as the point of contact for all pay adjustments, vacation requests, new hire information, address changes, benefit plans, etc. Guards should never call Head Office.
- All such requests or adjustments must be completed on the appropriate, approved SRG payroll forms and approved by the branch manager before submitting to the payroll administrator.
- All payroll forms must be submitted to the payroll administrator for processing no later than 12:00 noon on the Thursday prior to payroll submission. *Note: Payroll schedule/submission dates may be advanced during pay periods in which a statutory holiday occurs.*

Payroll Processing

- Payroll Detail by Employee reports must be reviewed for completeness and accuracy: Ensure all employee numbers are correct, all overtime is captured, and that pay rates and overtime rates/hours are correct.
- All payroll forms must be reviewed for completeness and accuracy: Ensure calculations are correct, time off or pay requests are within an employee's available accrual, etc.
- Payroll must be processed and submitted through Ceridian by no later than 5:00 PM every second Tuesday as per SRG's existing Ceridian payroll schedule. *Note: Payroll schedule/submission dates may be advanced during pay periods in which a statutory holiday occurs.*

Employee Pay Adjustments

- The designated branch point of contact should handle all calls/emails from employees and investigate whether a pay adjustment is required.
- Pay Adjustments must be completed and submitted on a Payroll Adjustment Form by the Operations Manager/Supervisor or the Scheduler and must be approved by the Senior Manager.
- Payroll Adjustment Forms should be sent immediately to the Payroll Administrator.

2. Management, Administration, and Cyber Division Payroll

Payroll Adjustments and Forms

- All such requests or adjustments must be completed on the appropriate, approved SRG payroll forms and approved by the appropriate division management before submitting to the payroll administrator.
- Cyber Security Division payroll forms must be approved by the Vice President, Cyber Security Services; Management and Administration payroll forms must be approved by the President & COO
- Approved payroll forms must be submitted to the payroll administrator for processing no later than three business days prior to the period pay date.

Timesheet Submission (Cyber Security Division)

- All Cyber Security Division employees must submit their hours worked on an approved SRG timesheet to the payroll administrator and copy the Cyber Division's SDO inbox.
    - Salaried employees must submit timesheets monthly at the end of the month, to be approved by the Vice President, Cyber Security Services.
    - Hourly employees must submit timesheets at each pay period ending as per the schedule provided by the payroll administrator, to be approved by the Manager of MSS.

Payroll Processing

- Paycheques are created in Sage Accounting.
- All adjustments and calculations are done manually and must be reviewed by the payroll administrator before submitting to the Finance Manager for processing.

Payroll Approval and Telpay Submission

- Payroll documentation (hard copy) is provided to the Finance Manager for review and approval. This includes completed pay stubs, a record of the payroll administrator's calculations, and Sage report showing the grand total in the payroll clearing account.
- The Finance Manager must provide an electronic payroll report to the President & COO for approval. Once approved, the Finance Manager submits the payroll to Telpay.
- A day before pay day, the payroll administrator emails pay statements to employees.

Change History

May 14, 2020 – Combined Payroll and Billing Policy split into separate policies. Additional details outlined; Procedures updated.

3000.30 Billing Administration

Effective Date:	**June 29, 2012**
Last Updated:	**May 13, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that invoicing functions, completed accurately and timely, will strengthen the overall financial health of the organization and will help maintain positive business relationships with customers. The intent of this policy is to establish standards for invoicing and to ensure consistency in the way all invoices are managed.

Guidelines

- Protective Services Division customers shall be invoiced every two-weeks following service/product delivery. Note: A monthly billing schedule may also be followed if specified by contract.
- Cyber Security Services Division customers shall be invoiced monthly following service/product delivery. Note: An annual or advanced billing schedule may also be followed if specified by contract.
- Protective Services Division (except SOC) invoicing is processed by the Payroll, Billing and Benefits Administrator for Protective Services; Cyber Security Services Division and SOC invoicing is processed by the Payroll, Billing and Benefits Administrator for Management and Cyber Division.
- All invoices are sent via email, unless otherwise requested in hard copy by the client.
- Failure to receive an invoice does not release a customer from their responsibility to pay. SRG's records of the date of emailing or mailing an invoice shall be conclusive evidence of the date of rendering.

Workplace Responsibilities

Management

- Ensure all new client, contract, and invoicing information is collected and submitted to the appropriate billing administrator in a timely and accurate manner on an approved Service Detail Report (SDR) form.
- Ensure any changes to client, contract, and invoicing information is collected and submitted to the appropriate billing administrator in a timely and accurate manner on an approved SDR form.
- Provide assistance or forward inquires to the billing administrator pertaining to remuneration concerns.

Billing/Finance Department

- Update and maintain the company's invoicing information system with new or updated customer information.
- Process invoices in a timely and accurate manner to ensure customers are invoiced accurately and on schedule.
- Provide accurate and timely report to the Finance Manager upon completion of invoicing.
- Respond to invoicing and payment inquiries from customers and management.
- Maintain confidentiality concerning customer invoicing information and remuneration.

SRG Security Resource Group Inc.

- Comply with all provincial, federal and legal invoicing requirements, duties and responsibilities pertaining to taxation and reporting.
- Create, maintain and update as required consistent and comprehensive invoicing processes and procedures.

Procedure

- New client, contract, and/or invoicing information as well as any changes to client, contract, and/or invoicing information must be submitted by the branch manager/administrator to the appropriate billing administrator as soon as possible in advance of the billing period ending on an approved SDR form.

- All invoices are to be processed in Sage (Simply Accounting program) and are to be emailed to customers as soon as possible following the end of the billing period (within the first business week if possible).

1. Protective Services Division (except SOC) Billing

Guard Services

- Approval to process billing be submitted to the billing administrator by Tuesday at 5:00pm Saskatchewan time following the period end.
- InTime reports to be used for billing are Margin by Customer and Billing Detail by Location. Total payroll number in the Margin by Customer report should be equal to the total payroll number in the Payroll Detail by Employee report.
- If a location is not billed, an explanation is required (i.e. Harvard retail sites are billed a monthly flat fee.)
- Margin by Customer report must be complete and accurate: ensure each location is billed, ensure rates are accurate and updated for new contracts, and if a location is not billed, insert an explanation onto report.

Mobile Services

- The Mobile Billing spreadsheet must be prepared by the designated branch administrator and submitted to the billing administrator by Tuesday at 5:00pm Saskatchewan time.
- Mobile Billing spreadsheet must be complete and accurate: The *Client Name* column should contain the customer's Legal Business Name, *Site* column should contain the address(es) where mobile checks are performed and the name of the building/park/pool if applicable, the billing rate and number of checks for each client must be correct, and the dates must be updated every period.

Alarm Services

- The Alarms Cover Sheet (summary) and the Occurrence Report (backup) forms must be submitted to the billing administrator by Tuesday at 5:00pm Saskatchewan time.
- Each Occurrence Report must be complete and accurate: The form should clearly identify the customer's Legal Business Name (no abbreviations) and the address of the alarm site.

2. Cyber Security Division and SOC Billing

ITS & MSS Services

- Invoicing instruction sheets for each new or updated contract, based on information provided in SDRs, are to be prepared by the Manager of Administration and approved by the contract owner.
- Approved invoicing instructions must be sent to the billing administrator as soon as possible following the end of the month along with approved list of repeat-invoices (no updates or changes to billing details).

SOC Services

- The SOC Supervisor must maintain the Monthly Camera Monitoring Report and submit to the Manager of Administration at the end of the month.
- Invoicing instruction sheets for each new or updated contract are to be prepared by the Manager of Administration based on information provided in the Monthly Camera Monitoring Report and in SDRs and must be approved by the contract owner.
- Approved invoicing instructions must be sent to the billing administrator as soon as possible following the end of the month along with approved list of repeat-invoices (no updates or changes to billing details).

3. Adjustments to Billing

- All requests for changes to invoices must be directed to the appropriate branch or division manager as well as to the appropriate billing administrator to investigate whether an invoicing adjustment is required.
- Should an adjustment to an invoice be required, a Billing Adjustment Form must be completed and submitted by the Manager/Supervisor or the Scheduler and approved by the Senior Manager.
- Billing Adjustment Forms should be sent immediately to the appropriate billing administrator.

Change History

May 14, 2020 – Combined Payroll and Billing Policy split into separate policies. Additional details outlined, Procedures updated.

3000.40 Accounts Receivable and Collections

Effective Date:	**May 14, 2020**
Last Updated:	**May 14, 2020**
Approved By:	**Blair Ross**

Purpose

SRG has adopted this policy to ensure that outstanding payments are recovered in an appropriate and timely fashion. As the inability or failure to effectively collect funds for products and/or services provided creates a financial strain on the organization, SRG will strive to ensure that all payments are received and credit extended is managed appropriately.

Guidelines

- SRG requires a written and signed agreement for services being provided and payment(s) required. Exceptions may be made for emergency security services provided there an email record of the agreement.
- In certain circumstances, a deposit from the customer may be required. Invoices to obtain a deposit payment are acceptable and encouraged.
- Customers with outstanding balances will be required to remit payments directly to Accounts Receivable. Revenues generated from invoices will be credited to the appropriate department. Any payments that have been erroneously sent to the originating department must be forwarded to Accounts Receivable for processing.
- SRG requires payment in full for all products and/or services rendered within 30 days from the invoice date or as otherwise agreed to in the contract.
- SRG will apply a service charge for all payments that are returned by the bank as NSF (non-sufficient funds).
- In the event of any dispute over charges, the originating division head or branch manager will be responsible for resolving the disputed charge(s).
- Accounts Receivable will implement appropriate collection efforts for outstanding account balances, e.g. phone calls, reminder notices, etc. following the procedures outlined below.

Procedure

- An updated AR listing is pulled from Sage on Wednesday of each week and emailed to the President & COO, Division and Branch management, and Finance office.
- Where an account with an outstanding balance fails to remit payment after 30 days or as otherwise agreed to in the contract, the accounts receivable department will email the customer's statement and reminder to remit payment.
- Where an account with an outstanding balance fails to remit payment after 30 days outstanding, the accounts receivable department will email the outstanding invoice(s) and statement to the customer, copying the Division head and the Manager of Administration, and will follow up with the customer by phone.
- Where an account with an outstanding balance fails to remit payment after 60 days outstanding, the accounts receivable department will escalate to the division head for further action/communication. Note: For Protective Services division, accounts receivable will also copy the President & COO on the request for escalation.
- A collections spreadsheet with notes on current activity will be emailed to the President & COO every two weeks, and will be reviewed at each bi-weekly Administration Meeting.

Uncollectible Accounts

In the event that a customer fails to respond to requests for payment, SRG will employ the services of a collections agency, or utilize other available legal options, at the direction of the President & COO.

Change History

<Summarize changes to the previous version.>

INFORMATION TECHNOLOGY

4000.10 Anti-Spam

Effective Date:	**October 1, 2014**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes spam can not only waste time but can also lead to potentially dangerous viruses. The intent of this policy is to create guidelines in order to prevent or reduce the amount of spam our employees are receiving at their company address, as well as to avoid spam related viruses which have the ability to cause widespread damage to our computers and networking systems.

Scope

This policy applies to all users with access to the SRG email systems.

Guidelines

- Employees must ensure that their anti-spam software is installed and up to date.
- Company e-mail addresses must be used only for business related purposes. Do not sign up for any mailing lists unless they are business related.
- Do not give your company address to any vendors.
- If you have already distributed your e-mail address for non-business-related purposes you must contact the company that is sending the e-mails and ask that they be sent to your personal e-mail address instead.
- Do not publish your e-mail address on blogs or webpages unless you have been given permission to do so, as this is where many addresses are “harvested” and sold to spammers.
- If you are sure that an e-mail that has been sent to your business e-mail address is spam, do not open it! Instead, block the address and delete the e-mail.
- If you are unsure about an e-mail address or you suspect that it is spam do not open it. Google the address and see if it leads to a business with which we do business, or if it is identified as a spam address. If it is the latter then follow the steps in the bullet above.
- If you have inadvertently opened a spam e-mail do not click on any part of the e-mail. Close, delete and block it immediately. Do not respond to the e-mail event to ask to be “removed from the list”. This just confirms to the spammers that it is an active e-mail and may lead to an increase in spam. Advise the Director of IT Security

Change History

May 1, 2020 – Updated statement of Scope and removed item from Guidelines.

4000.20 Computer Password

Effective Date:	**October 1, 2014**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG is committed to establishing and maintaining secure computerized resources. It is imperative that SRG computers, network resources and confidential data are protected. This policy has been adopted to define password requirements governing the use of SRG networks, computers, workstations and other devices and employee responsibilities to ensure the protection of personal and company information.

Scope

This policy applies to all users that have been granted SRG accounts.

Policy

Password complexity will be enforced through technological means where possible. Where it is not, employees utilizing company owned electronic devices, will ensure that, whenever possible, all SRG computers and other electronic devices are password protected.

Procedure

Password complexity standards will be established, and enforced through technological means, by the IT Department. In the absence of a documented standard the following minimum shall apply:

- Passwords are both alphabetic, and numeric, and contain no less than eight (8) characters. Ideally, symbols will also be integrated into company issued passwords.
- Passwords are changed quarterly or in cases where passwords may have been compromised, shall be changed immediately.

Employees shall ensure that:

- Passwords are kept memorized, and copies of the written password shall be kept in a secure location.
- No password is shared with another employee, client, member of the public or any other person except as directed by IT administrators and or appropriate company or legal authorities.
- When an employee believes his or her password has been compromised, he or she must contact the program administrator and report this immediately for the issuance of a new password.

Change History

May 1, 2020 – Updates Scope, Policy, and Procedure statements.

4000.30 e-Signature

Effective Date:	**October 1, 2013**
Last Updated:	**October 1, 2014**
Approved By:	**Blair Ross**

Purpose

SRG recognizes the importance of professional communication including that used with email therefore a consistent e-Signature for all SRG email account users is required.

Additionally, SRG recognizes that an email could erroneously be sent to the wrong recipient therefore a disclaimer message must be included.

Scope

This policy applies to all SRG employees whom have been provided with an SRG email account.

Policy

SRG e-Signatures must be consistent (Including bolding and colouring) for all SRG email account holders. This is to be used on any outgoing emails including Replies or Forwards. Cell numbers are to be included for anyone who needs to be accessible to the SRG clients or employees after regular business hours.

The following is an example of how it is to appear:

> **Blair W. Ross**
> President & COO
> **SRG Security Resource Group Inc.**
> 300-1914 Hamilton Street
> Regina, SK S4P 3N6
> Phone: 306-522-1677
> Cell: 306-533-5016
> Email: bross@securityresourcegroup.com
> Web: www.securityresourcegroup.com
>
> This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the sender. If you are not the named and intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Procedure

Update/Develop your e-Signature (with bolding and colours) in the Signatures section in Outlook.

The disclaimer can be found on the Z Drive and is titled **e-Signature Email Disclaimer Sep 2013**

Change History

<Summarize changes to the previous version.>

4000.40 Hands Free Cell Phone Usage

Effective Date:	**June 29, 2012**
Last Updated:	**June 29, 2012**
Approved By:	**Blair Ross**

Purpose

SRG recognizes the value of technology in enhancing employees' ability to perform their job effectively. Inappropriate use of information technology could expose the company to potential embarrassment and possible litigation.

Scope

This policy applies to SRG employees.

Legislative Context

The law prohibits all drivers from using hand-held cell phones to talk, text, email or surf the Internet while driving.

Policy

Employees that have been assigned mobile devices for SRG use are expected to adhere to the law. Where employees with assigned equipment can demonstrate their need for hands free usage as part of their employment, SRG will purchase and supply a Bluetooth headset or visor mount device.

Change History

<Summarize changes to the previous version.>

4000.50 Remote Access

Effective Date:	**October 1, 2014**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

To define standards for connecting to SRG's network from any host. These standards are designed to minimize the potential exposure to SRG from damages which may result from unauthorized use of SRG resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical SRG internal systems, etc.

Scope

This policy applies to all SRG employees, contractors, vendors and agents with an SRG-owned or personally-owned computer or workstation used to connect to the SRG corporate network. This policy applies to all types of remote access connections used to do work on behalf of SRG, including reading or sending email and viewing intranet web resources.

Policy

It is the responsibility of SRG employees, contractors, vendors and agents with remote access privileges to SRG's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SRG.

Procedures

- Secure remote access must be strictly controlled. Access control standards will be established, and enforced through technological means, by the IT Department. In the absence of a documented standard the following minimum shall apply: Access will be enforced via one-time password authentication or public/private keys with strong pass-phrases.
- At no time should any SRG employee provide their login or email password to anyone, not even family members.
- SRG employees and contractors with remote access privileges must ensure that their SRG-owned or personal computer or workstation, which is remotely connected to SRG's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Non-standard hardware configurations must be approved by SRG IT Services, and must be approved security configurations for access to hardware.
- All hosts that are connected to SRG internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.
- Personal equipment that is used to connect to SRG's networks must meet the requirements of SRG-owned equipment for remote access as set by standards determined by the IT department.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the SRG production network must obtain prior approval from the Vice President of Cyber Security Services.

Change History

May 1, 2020 – Updates to Scope, Policy, and Procedures statements.

4000.70 Shared Network Drive

Effective Date:	**October 1, 2014**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG provides network and cloud-based storage space for work-related materials and files. SRG employees will be required to manage their usage of the network, and maintain their files in an appropriate fashion. To avoid the over-burdening of this resource, we ask that our staff delete non-essential files, and avoid placing personal files on the network drive or in OneDrive.

Scope

This policy applies to all SRG employees with access to the shared network drive or OneDrive.

Guidelines

- The ability to add, remove and or modify files on the network storage and cloud-based drives will be limited to Authorized Users.
- Authorized SRG staff shall use the network storage or cloud-based drive for business purposes only, and will remove all personal items and unnecessary items.
- Where an SRG staff member requires more storage space than they have been allotted, they shall make a request to the IT Department.
- The IT Department shall review any requests for additional storage space and provide the additional space as appropriate.
- SRG employees are required to adhere to this policy, and the provisions made herein.

Network Storage Drive Maintenance

IT Department shall maintain the storage drive to ensure that it operates effectively, and shall ensure that the devices meet the requirements of SRG.

IT Department will conduct regular audits of the storage drive to remove outdated files in consultation with the President & COO and the authorized users.

Shared Files

IT Department shall create a “File Sharing” folder. All Authorized Users will have access to this folder for the purposes of sharing files amongst one another.

Files placed in the “File Sharing” folder will remain there on a temporary basis. Staff who will require this material for long periods should download it to their personal folders for long term storage.

IT Department shall backup and delete files in the “File Sharing” folder two weeks following placement in the folder.

IT Department will delete backup files after a three-month holding period.

Backup Schedule

All network drives will be backed up to an external hard drive once a month (during server maintenance). That external hard drive is kept off-site.

Email data is stored in the cloud.

Change History

May 1, 2020 – Updated back-up schedule.

4000.80 IT Acceptable Usage

Effective Date:	**June 29, 2012**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes the value of technology in enhancing employees' ability to perform their job effectively. Inappropriate use of information technology could expose the company to potential embarrassment and possible litigation.

Scope

This policy applies to SRG employees. The IT resources are deemed to include: telephones, cellular telephones, Blackberry equipment, fax machines, copiers, scanners, desktop, laptop computers and tablets. This policy ensures SRG is safeguarded by describing the security responsibilities of SRG personnel.

Notifications to Personnel

All personnel accessing SRG systems and networks must be aware of the following:

- Systems and networks are monitored to manage network traffic, ensure systems are operating as intended, detect faults, detect internal and external threats, and to ensure compliance with policies and standards.
- Special monitoring may be permitted without notice to the user where illegal or other unacceptable use is suspected. This special case monitoring must be authorized by the Vice President Cyber Security Services.

Types of Usage

Three usage types have been identified for SRG's IT infrastructure: core usage, incidental usage and unacceptable usage as defined below. Significant and/or repeated incidences of incidental or unacceptable usage by employees may result in disciplinary action up to and including termination.

Procedure

Activities for the three usage types include:

Core Usage

Core uses are activities required to conduct business for SRG. They assist in supporting employees in completing the tasks assigned to their positions. SRG's IT systems exist primarily to facilitate the company's core processes including:

- Internal e-mails
- Internet research
- Personal devices such as tablets, PDAs, and cellular phones
- Word processing
- Assembling spreadsheets
- Tracking data
- Payroll/accounting administration

Incidental Usage

Incidental uses are those that are neither explicitly permitted nor explicitly prohibited. Incidental applications never require any action or intervention by anyone at the workplace other than the user. Incidental usage that becomes an imposition on others or burdens the system is no longer incidental and is not permitted. Examples include:

- Brief, personal telephone usage
- Faxing personal travel plans
- Checking the internet for news while on rest break
- Texting while on break
- Using laptops and mobile devices for personal use
- Using internet to listen to music

Unacceptable Usage

Unacceptable uses impede the work of others and wastes IT resources. It may unintentionally damage the IT infrastructure and affect SRG's ability to carry out its work. Unacceptable uses may generate additional costs. Examples include:

- Using workplace technology for personal gain
- Using workplace technology for storing personal information not relevant to SRG/client
- Installing personal software on SRG/client owned equipment
- Adding personal software on SRG/client owned equipment
- Adding personal e-mail accounts on SRG/client owned equipment
- Distributing chain e-mails using SRG/client owned equipment
- Downloading/viewing music, videos etc. onto SRG/client technology
- Using internet access to watch videos on work time
- Using SRG/client telephones to dial inappropriate numbers or 1-900 numbers
- Downloading/viewing files from the internet that contravene SRG's Code of Conduct

Change History

May 1, 2020 – Updated with additional details of usage.

4000.85 Social Media Policy

Effective Date:	**April 24, 2020**
Last Updated:	**April 24, 2020**
Approved By:	**Blair Ross**

Purpose

This policy is in place to minimize the risks to SRG business through the use of social media. The policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia and all other social networking sites, internet postings and blogs. It applies to the use of social media for business purposes as well as personal use that may affect SRG business in any way.

Use of SRG Assets

Occasional use of social media from SRG assets is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

Representing SRG on Social Media

Personnel must not express opinions on behalf of SRG or include SRG branding, logos or other trademarks in any social media posting or in your profile on any social media, unless expressly authorised by the President.

Personal Conduct on Social Media

Personnel must not:

- make any social media communications that could damage SRG business interests or reputation;
- use social media to defame, disparage or impersonate SRG, co-workers, or any third party;
- harass, bully or unlawfully discriminate against colleagues or third parties; or
- post comments about sensitive business-related topics or do anything to jeopardise SRG confidential information and intellectual property.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your Manager.

Disciplinary Process

Employees in violation of security policies and procedures are subject to disciplinary actions as detailed in SRG policy manual section 2000.40, “Discipline”.

Change History

<Summarize changes to the previous version.>

4000.90 Web Mail Usage

Effective Date:	**June 29, 2012**
Last Updated:	**May 1, 2020**
Approved By:	**Blair Ross**

Purpose

SRG recognizes that inappropriate use of information technology could expose the company to potential embarrassment and possible litigation.

Scope

This policy applies to SRG employees and contractors. The IT resources are deemed to include: telephones, cellular telephones, Blackberry equipment, fax machines, copiers, scanners, desktop, laptop computers and tablets.

Policy

As there are security and records keeping issues with web-based mail accounts (e.g. Yahoo and Gmail), such accounts are not to be used for sending correspondence concerning SRG business, except where there are no other reasonable alternatives available.

Procedure

Where there are no other reasonable alternatives available, the sender is responsible for sending a copy of the email to an active account on SRG's server.

Change History

May 1, 2020 – Updated Scope and Policy statements.

MANAGED SECURITY SERVICE ENVIRONMENT

5000.10 MSS Personnel

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

In order to reduce the risk of human error, theft, fraud or misuse, SRG addresses personnel security with screening before granting access to the Managed Security Service (MSS) environment, and with responsibilities to safeguard assets while access is granted.

Job Commencement

Employees or contractors who will be granted access to the MSS environment require a satisfactory criminal background check, must have a confidentiality and non-disclosure agreement in place, and must receive a copy of the Managed Security Service Policies and have an opportunity to ask questions for clarification before access is granted.

Responsibility to Safeguard Assets

Employees, sub-contractors, and partners have a responsibility to safeguard sensitive information in their care. They must:

- ensure that only authorized individuals with a need-to-know have access to information in the MSS environment. They must not share passwords or leave unlocked computers unattended;
- not divulge any technical information to third parties without permission from the Vice President of Cyber Security Services or designate (such as the MSS Operations Manager or On-boarding and Project Services Manager) — examples include surveys, vendor inquires, questions about hardware/software platforms, questions from customers about other customers, etc; and
- report any issues that they are aware of to the MSS Operations Manager.

Disciplinary Process

Employees in violation of security policies and procedures are subject to disciplinary actions as detailed in SRG policy manual section 2000.40, “Discipline”.

Job Termination

Upon termination of employment or contract, all access privileges must be revoked.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.20 MSS Work from Non-SRG Location

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

SRG is committed to establishing and maintaining secure technology resources for the delivery of the Managed Security Service (MSS). One part of the service delivery model is the ongoing support provided from the MSS team members from a non-SRG location. As such, this policy provides the detailed requirements for the MSS team when working from a non SRG location.

Scope

This policy applies to all personnel involved with access to the secured MSS environment when working from a non-SRG location.

Policy

SRG resources that are part of the MSS offering for customers will ensure that all procedures are adhered to. If an exception is required that deviates from the procedures outlined below, formal permission from the Vice President, Cyber Security Services (or designate) is required including documentation on the exception.

Procedure

- Must use an SRG issued and managed computing asset for the delivery of the services.
- Must physically secure their non-SRG work environment (IE: separate locked room with controlled access) and ensure that guests are never left unattended in work environments where sensitive information may be physically viewed or logically accessed.
- SRG computers with access to the MSS environment are to be used only for official SRG-related work. These assets may not be used for personal purposes.
- Access to the secure MSS environment must be by the SRG-provided authentication and VPN technologies provided by SRG.
- Access to customer data is for MSS services only. MSS security team members are to adhere to all SRG policies including the executed employment confidentiality and non-disclosure documentation.
- As part of the annual performance review, MSS team members performing any customer work from a non-SRG work location agree to a physical review of the non-SRG environment by SRG. As well, random checks may be executed though out the work year.

Change History

Version	Summary of Changes
1.0	Initial version created November 2014 by Brian Zerr.
1.1	Modified January 2016 by Brian Zerr
1.2	Revised April 2020

5000.30 Information Classification & Control

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

Ensuring that sensitive information in the MSS environment is handled appropriately.

Scope

This policy applies to anyone with access to information in the MSS environment that is not their own information (i.e., client access to their own data is not in scope).

Sensitive Information

All information assets in the MSS environment are considered to be sensitive in nature and must be handled accordingly in order to safeguard its integrity and confidentiality.

As the MSS environment is inherently limited-access, there is no analogue to “public” information used by other classification schemes.

Information Handling and Test Environments

In addition to the standard secure handling of information that all information assets in the MSS environment receive, information assets may not be used unaltered in a test environment.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.40 Physical Security

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

To ensure that SRG MSS implements industry recommended physical and environmental controls to protect the assets of both itself and its clients, and further ensures that any 3rd party business partner that provides datacenter, network, or data management for SRG implements physical and environmental security controls that meet or exceed those defined in this policy.

Scope

The following physical and environmental controls must be present within any datacentres managed by SRG or its partners. Additionally, disaster recovery requirements must meet or exceed those outlined in SRG's BCP/DR Policy.

Physical Access to Datacentres

All datacentres must have controls to limit access to authorized personnel only.

Personnel Security

- Guards, cleaning staff, service engineers require criminal background checks that must comply with or exceed those outlined in the SRG Personnel Policy.
- All users of the facility and all building staff must sign non-disclosure agreements.
- Personnel must have ID badges and access cards.

Surveillance

Video surveillance must be implemented in room with no blind spots and further it:

- must be connected to back-up power; and
- must be monitored.

Datacentre Facility Construction

Redundant HVAC System Requirements:

- Temperature regulated between 55 and 75 degrees
- Humidity regulated between 20 and 80 percent
- Environmental sensors to alarm when levels are below or exceeding desired levels
- Air filtration

Fire Suppression Requirements:

- Gaseous fire suppression or other total flooding agent
- A fire extinguisher in every room
- Doors must be fireproof
- Fire/smoke monitoring

Electrical redundancy and battery back-up onsite with sufficient duration to switch over to diesel power generation.

Each data center room must have emergency power off switches for disconnecting power to SRG MSS hardware.

No unsecured windows to outside are to be located in datacentre.

All external walls in datacentre room must extend from floor to ceiling.

All access points must be posted with signs marking the room as restricted access and prohibiting food, drink and smoking.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.50 Operations Management

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

To ensure operational controls and process are in place to support the confidentiality, integrity, and availability of data service.

Scope

This policy applies only to the internal operations management of the MSS environment, and does not apply the corporate or client environments.

Inventory of Physical Assets

All SRG assets within the secured MSS environment must be inventoried in the MSS Document Management System.

Network Time

To assure network reliability and consistency, all network time on network devices, servers and SRG workstations will be synchronized from a trusted Network Time Protocol (NTP) source.

Logs

- SRG will collect, correlate, monitor, and archive all logs deemed pertinent to the ongoing administration of the MSS environment. These logs will be used by the MSS service with itself as a client, following standard processes and procedures as for other clients.
- Incidents initiated from findings during log monitoring and analysis will be categorized and dealt with according to the Incident Response procedure.

Incident Response Procedure

All internal MSS incidents escalated will be assigned a lead incident response analyst, who will transparently document the incident response and provide a post-incident report to the MSS Operations Manager.

Incidents must be categorized as Critical, Significant, or Low.

- Critical Incidents have the potential to affect the Confidentiality, Integrity and/or Availability of core network components and/or sensitive data.
- Significant Incidents have the potential to affect the Confidentiality, Integrity and/or the Availability of key business components and/or non-sensitive data.
- Low categorized Incidents have the potential to affect the Integrity and/or Availability of business components that are not key to day-to-day business.

All significant or higher incidents must have a post-mortem meeting to discuss prevention and mitigation techniques to prevent similar incidents in the future. The timelines of every finalized Incident Report will be analyzed for the purpose of incident response process improvement.

Capacity Planning

- Capacity planning exercises will be performed by the MSS On-boarding and Project Services Manager, as new clients and services are onboarded. Client onboarding processes must provide an analysis on the increase to capacity requirements of the SRG MSS infrastructure.
- The MSS Operations Manager will perform periodic long-term capacity monitoring and forecasting for peak capacity requirements of the technological infrastructure for day-to-day operations.

Software Patches

- Security patching of operating systems, applications, and software will be performed by SRG on a regular basis. Patches will be analyzed and applied using the Change Management procedure.
- Critical patches, or a technical work-around to announced vulnerabilities, must be applied to vulnerable software versions as soon as can be accommodated within the Change Management policy using the Emergency Change Control Procedures.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.60 Disaster Recovery

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

As SRG relies on information technology systems in order to perform day-to-day MSS operations and services, SRG must implement disaster recovery processes to assure minimal downtime of these IT systems in the event of unforeseen events or complete disaster.

Scope

This policy applies only to the secured MSS technical environment and does not apply the corporate or client environments.

Monitoring

SRG will ensure that monitoring is in place for all infrastructure so that issues can be detected. Alerts will be issued to the appropriate personnel for investigation.

Documentation

To avoid single points of failure with regard to personnel, all management personnel and team leads must ensure that all critical processes for which they are responsible are documented and made available to all SRG personnel with a legitimate need-to-know via the SRG MSS Document Management System.

System Backups

SRG must ensure that daily backups are taken of the hosted SIEMs and ELM DBs, as well as for supporting infrastructure such as Linux and Windows server VMs.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.70 User Access Control

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

In order to support the confidentiality, availability, and integrity of the MSS environment and the client data it supports, SRG implements strict security measures to ensure that user access is controlled.

Scope

This policy applies only to the secured MSS technical environment and does not apply the corporate or client environments.

Authorizing New Accounts and Groups

New user accounts, representing access by a new person, require approval of the Vice President of Cyber Security Services or designate (such as the MSS Operations Manager).

Least Privilege

SRG uses the security principle of “least privilege” – accounts created in the secure MSS technical environment must have the minimum level of access required to accomplish its business-related tasks as defined by its role.

Reviewing Access

The MSS Operations Manager must at least annually review all accounts to ensure that stale accounts have been removed and that access is appropriate for current job responsibilities.

Permitted Authentication Sources

Only SRG managed authentication services are permitted for accounts in the MSS environment.

Authentication Transmission

Authentication credentials must not be transmitted across the network in clear text and must use compliant encryption to protect the credentials while in transit.

Requirement for Passwords – External Access, Two-factor

External access into the MSS environment requires two-factor authentication, with technologically enforced standards for the two-factor authentication as determined and documented by the MSS Architect.

Requirement for Passwords – Single-factor, Internal-only Access

To accommodate internal tools that are unable to support two-factor authentication for services that can only be reached internally after having already authenticated using another method (i.e. the user must first VPN into the environment or access an externally-accessible jump box), single-factor authentication for individual tools is permissible using authentication with technologically enforced standards as determined and documented by the MSS Architect.

Requirement for Passwords – Service Accounts

- Standards for service accounts are as determined and documented by the MSS Architect.
- In the absence of any documented standard for service accounts to the contrary, they may be set to not require password expiry if they have interactive logins technologically disabled.

Requirements for Password Resets

Password resets require that the account owner authenticate themselves in-person or by voice from a phone number known to be associated with them to the MSS support personnel performing the password reset.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.80 Network and System Access Control

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

In order to support the confidentiality, availability, and integrity of the MSS environment and the client data it supports, SRG implements strict security measures to ensure that network and system access is controlled.

Scope

This policy applies only to the secure MSS technical environment and does not apply the corporate or client environments.

Default Deny

Firewall rules will be written and implemented in accordance with the Principle of Least Privilege. No firewall rules will be written to a firewall ruleset that allow unrestricted port access.

Segregating Networks

Firewalls will be implemented between the MSS environment, the SRG corporate network, and all client networks.

Site-to-Site VPNs may be created for the purposes establishing persistent connections between SRG and its clients to enable client data to be ingested by SRG Managed Security Services. VPN tunnels will be configured to only permit traffic that enables the services agreed to and outlined in the services contract between SRG and its clients. All other network traffic will be denied. Further, routing between site-to-site VPNs must be specifically prevented.

Requirement to use Change Management for Firewall Rule Changes

Firewall rules will not be written to a firewall ruleset without first being approved by the Change Management process.

Vendor Remote Access

3rd party vendors requiring remote access in order to provide support to SRG will be granted remote access only during those periods where they will be connected to the network. All 3rd party vendor access must be monitored by SRG personnel. 3rd party vendor access permissions will be disabled when the vendor is not connected to the network.

Customer Access to MSS Environment

Customer access may be enabled by web portals that will allow a customer to view their data. Customers will be limited to viewing their own data and will not have admin or write access to SRG systems.

Test Environments

Unless required and approved by the Change Management process, test systems will not be granted ingress or egress access to the Internet.

Test environments must be segregated from all production environments. Test environments must only be accessible by those who are performing the testing or developing the test environment.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

5000.90 Cryptography

Effective Date:	**April 27, 2020**
Last Updated:	**April 27, 2020**
Approved By:	**Blair Ross**

Purpose

To provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Scope

This policy applies only to the MSS technical environment and does not apply the corporate or client environments.

Permittable Algorithms and Ciphers

All encryption used for the MSS environment should use common, well-understood ciphers as compliant with FIPS 140-2[1] (or newer).

The use of proprietary encryption algorithms are not permitted for any purpose, unless reviewed by the MSS Architect and approved by the SRG On-boarding and Project Services Manager.

Secure Data Handling

The use of compliant cryptographic controls for data in transit is required when:
- the traffic in question carries any sort of authentication or authorization information;
- the traffic in question involves administrative control (privileged access) to network or server equipment for system management purposes;
- the traffic in question involves any sort of remote access across the MSS logical security perimeter; or
- an agreement with a client or partner requires it.

The use of compliant cryptographic controls for data at rest is required when:
- backups are stored off-site;
- portable storage devices designated as intended to hold MSS data; or
- an agreement with a client or partner requires it.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

[1] http://csrc.nist.gov/groups/STM/cmvp/standards.html

5000.100 Change Management

Effective Date:	**April 28, 2020**
Last Updated:	**April 28, 2020**
Approved By:	**Blair Ross**

Purpose

In order to maintain a comprehensive understanding of the components and intricacies of a networked computing environment, all changes to the MSS environment must be controlled and documented.

Scope

This policy applies only to the MSS technical environment below the level of the SIEM interface and does not apply to:

- non-technical changes (such as documentation);
- the corporate technical environments; or
- client technical environments before the SRG/client demarcation line; or
- co-managed environments where the customers change management process is utilized.

Changes within the SIEM interface, such as data source MACD and parsers, do not use the Change Management process and are instead tracked using regular MSS tickets that are assigned to the client department.

Similarly, Use Cases within the SIEM have their own quality assurance and change procedure documented in the MSS Document Management System and are out-of-scope for this policy.

Change Management Procedural Documentation

Current procedural documentation must be maintained in the MSS Document Management System.

Change Submitters and Implementers

Any SRG MSS personnel may submit a Change Request (CR) using the current procedure documented in the SRG MSS Document Management System. To ensure that the CR is submitted and implemented correctly, the Change Submitter is also the Change Implementor unless an exception is approved by the MSS Operations Manager.

Change Approvers

The MSS Operations Manager will ensure that multiple senior personnel are assigned the role of Change Approver, and that the list of Change Approvers is part of the documented procedure.

The Change Approvers review submitted CRs and either approve, deny, or provide feedback for the CR.

Customers will not be consulted for technical approval of CRs.

Restrictions on Change Approval

Change Requests require two approvals in order to proceed. Change Approvers may not approve their own CRs.

A CR will not be approved by SRG Change Approvers members without the following information:

- a clear description of the change;
- a full implementation plan;

- a back-out plan explaining how to revert the component or system back to the documented baseline if the change fails; and
- a scheduled time for the change implementation.

Change Request Impact Categorization

Changes will be categorized by their impact to the SRG MSS environment and clients. CR submitters will determine the CR impact categorization based on the following criteria:

1. High: These changes have high impact on the environment, could affect most of the environment, and will, or possibly could, cause service downtime or data loss for multiple customers.
    a. High Impact CRs should be implemented outside SRG and impacted customer core business hours where possible.
    b. Clients must receive notification of the scheduled downtime 3 business days prior to the implementation of the CR and client approval for the scheduled change time should be obtained if possible.
2. Significant: These changes have a high impact on the environment, will affect at least 1 customer, and will, or possibly could, cause network service downtime or data loss for a customer.
    a. Significant CRs should be implemented outside the impacted customer core business hours where possible.
    b. Clients must receive notification of the change implementation at least 2 business days prior to the implementation of the CR.
3. Low: These changes will not have much impact on the environment and are not likely to cause service downtime.
    a. Low impact CR's should be performed outside of core business hours where possible.
    b. Clients do not need to be notified of low impact changes.
4. Emergency: Emergency Changes will be scheduled and performed as part of the incident response process.
    a. Emergency changes will be performed as required.
    b. Emergency Changes will be documented and reviewed at next scheduled senior analysts or division management meeting.

MSS Customers

If an MSS customer requires custom change management procedures, a documented agreement must be made between SRG and its customer that will outline the service needs. If a CR is submitted and approved that may impact these defined service needs, SRG will contact the client prior to implementation and within the terms of the contingencies outlined in the agreement.

Test Environments

A test environment may be established as needed and changes made to it without requiring CAB approval as long as it meets all other policies.

The use of a test environment is discretionary for changes that do not have an Impact classification of High.

Change Implementation

Change Implementers will ensure:

- only the work outlined in the implementation plan will be performed;
- work will only be performed within the scheduled change window – this includes back-out work, if required; and
- if a back-out plan change fails, the emergency change request process will be followed to ensure the documentation of any changes not outlined in the original Change Request.

Finalization

If the Change is successful, all Change Requests must be finalized by marking the change request ticket as closed. All system documentation is to be updated to the newest versions and these versions will become the new baselines for that system or component.

If the change fails, the system must be reverted back to its most recent baseline. If any additional work was performed in addition to that outlined in the CR back-out plan to restore the system or component to its most recent baseline, that work must be documented in an emergency change implementation plan. Failed changes with High or Significant changes must be communicated to the client and rescheduled once the Change Implementor has developed a new implementation plan.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency. Sub-sections that are no longer relevant were removed.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices. Updated the Scope to exclude certain items that are handled through a different process. Updated Test Environments.

5000.110 Physical Media and Data Destruction

Effective Date:	**April 28, 2020**
Last Updated:	**April 28, 2020**
Approved By:	**Blair Ross**

Purpose

As information which is inadvertently left on media could potentially cause unauthorized disclosure or use of sensitive information, all permanent or temporary media for information processing systems must be sanitized from SRG MSS equipment before such equipment is permanently transferred outside of SRG or disposed of in any other means.

Scope

This policy applies only to the MSS technical environment and does not apply the corporate or client environments.

Secure Sanitization

Secure media sanitization options that are considered compliant include:

- using a software-based secure data erasure that uses the CSEC ITSG-06[2] Data Wipe Method or the very similar NAVSO P-5239-26 and DoD 5220.22-M 3-pass methods;
- the Secure Erase set of hardware commands built into the firmware of PATA and SATA based hard drives; and
- for devices containing non-removable media, the use of physical destruction.

End of Life

Electronic devices and storage media that were encrypted according to the Cryptography Policy section do not require data destruction in the event of non-routine end-of-life situations (such as hardware failure).

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.

[2] http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html

5000.120 Compliance

Effective Date:	**April 28, 2020**
Last Updated:	**April 28, 2020**
Approved By:	**Blair Ross**

Purpose

The MSS service must ensure compliance with applicable legislation, regulatory requirements, and 3rd party contractual agreements.

Scope

This policy applies only to the MSS technical environment and does not apply the corporate or client environments.

Conflict in Compliance Requirements

In the event that there exists a conflict in compliance requirements, a “high water mark” method is used such that the most stringent requirement for a given situation will be followed.

Intellectual Property Rights and Licensing

Terms and conditions of all software End User License Agreements are to be strictly adhered to in order to comply with copyright legislation and to ensure ongoing vendor support.

Third-Party Agreements

- Non-disclosure and confidentiality clauses must be present in all 3rd-party contracts that would result in access to the MSS environment. Technical security concerns are addressed prior to providing connection/access to external parties/customers.
- Ensuring compliance with SRG MSS security policies and standards must be formally addressed in agreements with datacenter partners.

Communicating Policy

The Vice President of Cyber Security Services (or their delegate) ensures that employees, contractors, and partners with access to the MSS environment are annually made aware of and provided access to the SRG MSS policy manual and any 3rd-party contractual requirements that they are required to uphold.

Change History

Version	Summary of Changes
1.4	Initial version (2014).
1.5	Revised July 2019 to reflect evolving MSS practices. Minor wording revisions made throughout the document, especially as relating to consistency.
1.6	Revised April 2020 to bring into line with SRG policy & procedures manual formatting. Minor wording revisions made throughout to update to match current practices.