3. CONFLICT OF INTEREST

The honesty and integrity of CSI Pacific demands that the impartiality of staff members, in the conduct of their duties, be above suspicion. Staff conduct should instill confidence and trust and must not bring our organization into disrepute.

Conflicts of Interest
A conflict of interest occurs when a staff member's private affairs or financial interests are in conflict, or could result in a perception of conflict, with the employee's duties or responsibilities

If a staff member is approached by a partner organization of CSI Pacific to perform duties over and above their responsibilities with the Institute the proposal must be presented to the CEO and the process of payment for these services will be agreed upon on a case by case basis. In some situations the partner organization will pay CSI Pacific who will pay the staff member, in other situations they may pay the staff member directly. Regardless of the scenario it must be agreed upon between the CEO and staff member.

Staff with questions regarding interpretation of the policy may discuss them with their Lead and consult the Controller. Staff who find themselves in an actual, perceived or potential conflict of interest must disclose the matter to their Lead immediately. Staff who fail to disclose may be subject to disciplinary action up to and including dismissal.

Examples of conflicts of interest include, but are not limited to, the following:

- a staff member uses CSI Pacific property or the staff member's position or affiliation to pursue personal interests;
- a staff member is in a situation where he/she is under obligation to a person who might benefit from or seek to gain special consideration or favour;
- a staff member, in the performance of official duties, gives preferential treatment to an individual, corporation or organization, including a non-profit organization, in which the staff member, or a relative or friend of the staff member, has an interest, financial or otherwise;
- a staff member benefits from, or is reasonably perceived to have benefited from, the use of information acquired solely by reason of employment;

- a staff member benefits from, or is reasonably perceived to have benefited from, a transaction over which the staff member can influence decisions (for example, sales, purchases, contracts, or appointments);
- a staff member requests or accepts from an individual, corporation or organization, directly or indirectly, a personal gift or benefit that arises out of their employment other than:
- the exchange of hospitality between persons doing business together;
- tokens exchanged as part of protocol;
- the normal presentation of gifts to persons participating in public functions;
- the normal exchange of gifts between friends; and
- a staff member solicits or accepts gifts, donations or free services for work-related leisure activities other than in situations outlined above.

Outside Remunerative and Volunteer Work
Staff may engage in remunerative employment with another employer, carry on a business, or engage in volunteer activities provided it does not:

- interfere with the performance of their duties;
- bring CSI Pacific into disrepute;
- represent a conflict of interest or create the reasonable perception of a conflict of interest;
- involve the unauthorized use of work time or premises, services, equipment or supplies to which they have access by virtue of their employment; and
- gain an advantage that is derived from their employment as an employee.

Confidentiality and Intellectual Property
All staff and contractors sign a Confidentiality and Intellectual Property Agreement before commencing employment. Any exceptions or changes to the agreement must be approved by the CEO. Generally, intellectual property, copyrights, patents, and trademarks resulting from the staff member's professional work on behalf of CSI Pacific become the property of CSI Pacific unless otherwise permitted by written agreement. Confidential information that staff receive through their employment must not be divulged to anyone other than persons who are authorized to receive the information. Confidential information that staff receive through their employment must not be used by a staff member for the purpose of furthering any private interest, or as a means of making personal gains. Staff who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing it. Caution and discretion in handling confidential information continues to apply after the employment relationship ceases.

Items purchased by CSI Pacific or produced by employment duties are the sole property of CSI Pacific and may only be removed from CSI Pacific premises for work related purposes, may not be copied for personal use or given to another party.

Public Comments
All requests for public comment regarding the policies or operations of CSI Pacific are to be referred to the staff member's Lead.

Political Activity
Staff are free to participate in political activities including belonging to a political party, supporting a candidate for elected office and actively seeking elected office. Staff members' political activities, however, must be clearly separated from activities related to their employment. If engaging in political activities, staff must be able to retain the perception of impartiality in relation to their duties and responsibilities to CSI Pacific. Staff must not engage in political activities during working hours and partisan politics at the local, provincial or national levels are not to be introduced into the workplace. This does not apply to informal private discussions among co-workers.

Allegations of Wrongdoing

Staff have a duty to report either to the CEO or, in the event of the alleged involvement of the CEO in the concern, to the Chair of CSI Pacific; any situation that they believe contravenes the law, misuses funds or assets, or represents a danger to public health and safety or poses a significant threat to the environment. Staff can expect such matters to be treated in confidence, unless disclosure of information is authorized or required by law (for example, the Freedom of Information and Protection of Privacy Act). Staff will not be subject to discipline or reprisal for bringing forward to the CEO, in good faith, allegations of wrongdoing in accordance with this policy.

Staff must report a safety hazard or unsafe condition or act in accordance with the provisions of the WCB Occupational Health and Safety Regulations.

Working Relationships
Staff who are direct relatives or who permanently reside together may not be employed in situations where:

- a reporting relationship exists where one staff member has influence, input or decision-making power over the other staff member's performance evaluation, salary, premiums, special permissions, conditions of work and similar matters; or
- the working relationship affords an opportunity for collusion between the two staff members that would have a detrimental effect on CSI Pacific's interest.

The above restriction on working relationships may be waived provided that the CEO is satisfied that sufficient safeguards are in place to ensure that CSI Pacific's interests are not compromised.

Personnel Decisions
Staffs are to disqualify themselves as participants in personnel decisions when their objectivity would be compromised for any reason or a benefit or perceived benefit could accrue to them.

- Loss of any item should be reported immediately to the Coordinator, Human Resources & Administration.

Key Control System

- Keys are under the management of CSI Pacific. All keys are identified by an engraved or stamped number and will be allocated to staff through their Lead.
- Office and campus keys may not be duplicated and lost keys must be reported immediately to the Lead.

Property & Equipment Security

It is important that all CSI Pacific personnel comply with the following security guidelines when working with property and equipment out of office and/or at training sites.

Staff are expected as part of their employment to safeguard CSI Pacific property and equipment, and property and equipment entrusted by CSI Pacific, from loss, theft or damage by taking reasonable steps such as, but not limited to:

- maintaining an accurate equipment inventory;
- keeping items protected from the elements, hazardous environments or conditions that might reasonably be expected to cause damage to the equipment;
- Using the equipment item in accordance with manufacturer's guidelines and only for the purpose(s) for which the item was designed;
- Ensuring required / preventative maintenance is performed;
- Securing equipment when not in use; and
- Limiting equipment access to CSI Pacific staff members trained in the use of the equipment.

Property and equipment is not to be left in a locked or unlocked Canadian Sport Institute Pacific or staff vehicle such that it is visible to an outside observer. Such equipment shall be moved to a secure Canadian Sport Institute Pacific location, a temporary storage facility or secure compound.

Loss or damage to any item shall be reported immediately to the Coordinator, Human Resources & Administration and the staff member's Lead. The staff member reporting such a loss shall, as soon as practicable, provide the Coordinator, Human Resources & Administration with a written statement outlining the circumstances that led to said damage / loss. Note: In cases of damage caused by fair wear and tear the Lead may waive the requirement to provide a written statement.

In cases where property and equipment is lost or damaged as a result of nefarious circumstances the staff member responsible for the equipment at the time of said occurrence shall cooperate fully with authorities and provide any information said authorities may require.

Where a staff member is found to be grossly negligent in caring for equipment entrusted to them, and such negligence contributes to a loss, the staff member may be held financially liable and / or be subjected to a disciplinary process.

5. WORKPLACE BEHAVIOR POLICY

All staff have the right to expect, and the responsibility to create, a workplace where all staff are treated with respect and dignity. Therefore, the conduct and language of staff in the workplace will meet acceptable social standards and will contribute to a positive work environment. A staff member's conduct will not compromise the integrity of CSI Pacific and staff will adhere to the Staff Code of Conduct policy.

Any form of violence, workplace bullying, harassment of any kind or discriminatory act toward any individual by employees, managers, contractors or any other stakeholder involved with CSI Pacific is taken seriously by CSI Pacific.

Definitions

Discrimination is an action or a decision that treats a person or a group negatively for reasons based on any of the prohibited grounds covered by the Human Rights Code. The prohibited grounds are race, colour, ancestry, place of origin, religion, family status, marital status, physical disability, mental disability, sex, sexual orientation, age, political belief or conviction of a criminal or summary offence unrelated to the individual's employment.

Workplace Bullying and Harassment includes any inappropriate conduct or comment by a person towards a worker that the person knew or reasonably ought to have known would cause that worker to be humiliated or intimidated.

Sexual Harassment includes any behaviour involving unwelcome sexual advances, requests for sexual favors or other communication (verbal or written) or physical conduct of a sexual nature that the person knew or reasonably ought to have known would cause that worker to be embarrassed, humiliated, offended and/or intimidated. Any abuse of power in exchange for sexual favours is considered sexual harassment.

Another form of bullying and harassment at work is ***Cyber-Bullying*** through electronic communications, i.e. e-mail, text messaging, social networking and websites. Sending derogatory or threatening messages or sharing personal and confidential messages or images are examples which will not be tolerated.

Bullying and harassing behaviours do not include:

- expressing differences of opinion
- offering constructive feedback, guidance or advice about work-related behavior; or
- reasonable action taken by an employer or supervisor relating to the management and direction of workers or the place of employment (e.g. managing a worker's performance, taking reasonable disciplinary actions, assigning work)

Violence in the workplace is also unacceptable and will not be tolerated. Violence is the attempt to exercise physical force against a worker, in a workplace, that causes or could cause physical injury to the worker.

Staff Responsibilities

Staff must:

- not engage in workplace behaviour that includes discrimination, bullying or harrassment
- report if discrimination, bullying or harrassment is observed or experienced; and
- apply and comply with the employer's policies and procedures on workplace behaviour

Workplace Behaviour Complaint Procedures

Staff must report any incident of workplace bullying, any type of harassment, discrimination or violence directed towards themselves or their co-workers. Any staff member seeing, hearing or experiencing any type of discrimination, bullying, harassment, or violence, in the workplace must report it if he or she has reasonable cause to believe that the threat is serious. Any incident that violates this policy must be addressed immediately.

CSI Pacific will treat staff complaints/reports in the strictest confidence. A staff member who believes that he or she has been affected in violation of this policy should submit a complaint using the *Discipline, Complaints and Dispute Resolution Policy*.

Workplace Restoration – Moving forward after complaints
After a complaint and investigation of inappropriate workplace behaviour has been conducted, it can be challenging for all those involved to move forward and restore workplace relationships. Whether the accusations were found to be true and discipline has taken place, or the claims were unsubstantiated, in many cases employees will need to continue working with one another, possibly with “hard feelings” of resentment and tension in the working relationship. During the investigation, words have been spoken and emotions have been exposed by all parties, including those that have been involved in the investigation (i.e. witnesses).

CSI Pacific will take a proactive approach in assisting staff in re-establishing their working relationships with one another and moving past the complaint and investigations that have taken place.

DISCIPLINE, COMPLAINTS & DISPUTE RESOLUTION POLICY

Approved September 19, 2014

Canadian Sport Institute Pacific (CSI Pacific) supports an environment of safety, trust and mutual respect for all its Staff. CSI believes that conflict brings an opportunity for change and greater understanding, and encourage all Staff to communicate openly, collaborate, and use problem-solving and negotiation techniques to resolve their differences.

Regrettably, not all conflict can be resolved through direct and open communication and formal procedures are necessary to resolve the complaint. In situations where serious conflict exists and intervention is necessary the following procedures have been put in place, in an effort to resolve conflict in an expedient, yet fair manner.

POLICY STATEMENT

Any breaches of CSI Pacific Policy, in particular those related to *Staff Code of Conduct, Board & Volunteer Code of Conduct,* and *Human Resources Policies* shall be handled using the following procedures.

DEFINITIONS

The following terms have these meanings in this Policy:

a) *"Clients"* – Users of CSI Pacific services, including on-site services, such as athletes, coaches, medical staff, and other personnel connected to a team or athlete;
b) "*Staff*" – Any individual employed by, or engaged in activities on behalf of, CSI Pacific including employees, contract personnel, volunteers, medical personnel, researchers, and administrators
c) "*Complainant*" – The Party initiating a complaint;
d) "*Days*" – Days irrespective of weekend and holidays;
e) "*Respondent*" – The Party who is the subject of the complaint; and
f) "*Parties*" – The Complainant, Respondent, and any other Individuals or persons affected by the complaint.

APPLICATION

CSI Pacific will provide an environment in which all clients and staff involved with CSI Pacific are treated with respect. Association with CSI Pacific, as well as participation in its activities, brings many benefits and privileges. Staff are expected to fulfill certain responsibilities and obligations including complying with CSI Pacific's policies, bylaws, rules and regulations, and *Staff Code of Conduct*. Irresponsible behaviour by staff can result in severe damage to the integrity of the CSI Pacific. Conduct that breaches these values may be subject to disciplinary action pursuant to this Policy. Since discipline may be applied, CSI Pacific provides staff with the mechanism outlined in this Policy so that complaints are handled fairly, expeditiously, and affordably.

This Policy applies to all staff, Board members, directors and volunteers. Complaints against clients will be directed to the client's National or Provincial sport organization, as appropriate.

This Policy applies to disciplinary matters that may arise during the course of CSI Pacific business, activities, and events including, but not limited to:

- contact with clients;
- travel associated with CSI Pacific activities;
- CSI Pacific's office environment, and;
- any business activities related to CSI Pacific.

Disciplinary matters and complaints arising within the business, activities, or events organized by entities other than CSI Pacific will be dealt with pursuant to the policies of these other entities unless requested and accepted by CSI Pacific at its sole discretion.

PROCEDURES

1. INFORMAL COMPLAINT PROCESS

It is our intention that employees will use open communication and attempt to resolve issues of conflict using the Informal Procedures and Alternate Dispute Resolution techniques before issuing a formal complaint.

Individuals are first encouraged to take initial steps to speak to the person they are having concerns with. Many times disputes arise due to misunderstandings and miscommunications.

If the request is unsuccessful, or if it is considered inappropriate or uncomfortable to make such a request, employees should discuss the matter with their Discipline Area Lead, or if the Discipline Area Lead is allegedly involved, to the Chief Executive Officer (or designate).

Alternative Dispute Resolution and Mediation
CSI Pacific supports the principles of Alternate Dispute Resolution (ADR) and is committed to the techniques of negotiation, facilitation, and mediation as effective ways to resolve disputes. Alternate Dispute Resolution avoids the uncertainty, costs, and other negative effects associated with lengthy appeals or complaints, or with litigation.

Opportunities for Alternate Dispute Resolution may be pursued at any point in a dispute within the Canadian Sport Institute Pacific when all parties to the dispute agree that such a course of action would be mutually beneficial.

2. FORMAL COMPLAINT PROCEDURES

Before issuing a formal complaint, staff should attempt to resolve the issue using the Informal Complaint Process. If the issue is not satisfactorily resolved, or requires a formal complaint to be issued, the following process should be followed:

1. The complainant will submit a formal complaint in writing, using the Formal Complaint Form, to the Chief Executive Officer (or designate), or where the Chief Executive Officer is involved, the Board, within ten (10) days of the latest alleged occurrence. Such a complaint must be in writing.
2. The Chief Executive Officer (or designate) will review the formal complaint and facts that have become known through the Informal Complaint Process and the Alternate Dispute Resolution Process (if applicable), who will determine the appropriate action to be taken such as disciplinary action, external mediation, or an investigation; and
3. A Complainant wishing to file a complaint outside of the ten (10) day period must provide a written statement giving reasons for an exemption from this limitation. The decision to accept, or not accept, the complaint outside of the ten (10) day period will be at the sole discretion of Chief Executive Officer (or designate) of CSI Pacific. This decision may not be appealed.

3. INVESTIGATION PROCEDURES

The process for investigations includes the following steps:

1. The Chief Executive Officer (or designate) will be responsible for initiating an in-house investigation at once in all cases of inappropriate workplace behaviour. The course of the investigation might involve outside authorities;
2. The investigator appointed will determine a fair and unbiased process to follow.

3. If the complainant and the respondent agree on what happened, then the investigator may not have to investigate any further;
4. All investigations will result in a written report with recommendations for resolution to the Chief Executive Officer (or designate), or the Board, as the case may be, who will inform the relevant parties of the final decision;
5. If the evidence found in the investigation upholds the allegation of inappropriate workplace behaviour, CSI Pacific shall initiate immediate follow-up and disciplinary action (as appropriate).; and
6. Reports of violence, discrimination, bullying or harassment found to be frivolous, vindictive, or vexatious in nature, may lead to disciplinary action.

4. DISCIPLINARY ACTION

The Chief Executive Officer (or designate) may apply disciplinary action depending on the seriousness of the incident.

5. CONFIDENTIALITY

The discipline and complaints process is confidential and involves only the Parties, the Investigator, the Chief Executive Officer (or designate), and any independent advisors to the Chief Executive Officer (or designate). Once initiated and until a decision is released, none of the Parties will disclose confidential information relating to the discipline or complaint to any person not involved in the proceedings.

6. TIMELINES

If the circumstances of the complaint are such that adhering to the timelines outlined by this Policy will not allow a timely resolution to the complaint, the Chief Executive Officer (or designate) may direct that these timelines be revised.

7. RECORDS AND DISTRIBUTION OF DECISIONS

All incidents that result in disciplinary action shall be recorded and maintained by CSI Pacific. Other Canadian Sport Institutes/Centres may be advised of any decisions.

NETWORK, COMPUTER EQUIPMENT & E-MAIL ACCEPTABLE USE POLICY

Approved December 4, 2015

POLICY STATEMENT

The Network, Computer Equipment and Electronic Mail (E-Mail) Acceptable Use Policy defines and outlines acceptable use of these resources at the Canadian Sport Institute Pacific (CSI Pacific). These rules and guidelines are in place to protect both the user and CSI Pacific. This policy requires all CSI Pacific staff and other users to comply with the acceptable use provisions.

DEFINITIONS

The following terms have these meanings in this Policy:

a) "*Staff*" – Any individual employed by, or engaged in activities on behalf of, CSI Pacific including: employees, contract personnel, volunteers, medical personnel, researchers, and administrators;
b) "*Clients*" – Users of CSI Pacific services, including on-site services, such as athletes, coaches, medical staff, and other personnel connected to a team or athlete; and
c) "*Workplace*" – Any place where business or work-related activities are conducted. Workplaces include but are not limited to, the CSI Pacific campus locations, work-related social functions, work assignments outside of CSI Pacific campus locations, work-related travel, and work-related conferences or training sessions.

APPLICATION

This policy applies to all offices and users, including employees, contractors, consultants, temporary staff, volunteers and other workers within CSI Pacific. This policy applies to all resources and information technology equipment owned or leased by the CSI Pacific regardless of the time of day, location or method of access.

Each office is responsible for assuring that staff and users under their authority have been made aware of the provisions of this policy, that compliance by the staff is expected, and that intentional, inappropriate use of network and e-mail resources may result in disciplinary action up to and including dismissal. To demonstrate awareness and knowledge of this policy, signed acknowledgement forms are required. It is also each Lead's responsibility to enforce and manage this policy.

PROCEDURES

1. APPROPRIATE USE OF NETWORK, COMPUTER EQUIPMENT, AND E-MAIL RESOURCES

As provisioned, network (including Internet), computer equipment and e-mail resources, services and accounts are the property of the CSI Pacific. These resources are to be used for CSI Pacific business purposes in serving the interests of CSI Pacific, its athletes, coaches and staff in the course of normal business operations. This policy represents a set of rules and guidelines to be followed when using the network facilities provided by CSI Pacific, including Internet and e-mail.

In compliance with the laws of the Province of British Columbia and this policy, staff of CSI Pacific is encouraged to use network, computer equipment and e-mail resources to their fullest potential to:

- Further CSI Pacific's mission
- To provide service of the highest quality to its clients
- To discover new ways to use resources to enhance service, and
- To promote staff development

CSI Pacific staff should use network, computer equipment and e-mail resources, when appropriate, to accomplish job responsibilities more effectively and to enrich their performance skills.

The acceptable use of network, computer equipment and e-mail resources represents the proper management of a CSI Pacific business resource. The ability to connect with a specific Internet site does not in itself imply that a staff member is permitted to visit that site. Monitoring tools are in place to manage and troubleshoot the network, servers and critical applications such as email. Due to these tools, all data on staff's Internet usage history, email, and data stored on CSI equipment such as computers and laptops can potentially be accessed when deemed necessary by business requirements. Therefore, staff should be aware there is no expectation of privacy associated with any of these activities.

Documents and files produced by staff and others working for CSI Pacific are the property of CSI Pacific and must be properly stored and backed up. Network drives are provided for the storage of documents and files related to a staff member's work at CSI Pacific. It is expected that staff will use the appropriate network location for saving files related to their employment. Work related files are not to be saved to the user's local computer, with the exception of users working remotely with no Internet connection. In this case, all data should be stored in "My Documents" folder (which will be automatically backed-up when an Internet connection is established, preventing loss of work). Once the user has a reliable Internet connection, he/she should copy the files to the designated shared folder in the corporate server for safe keeping.

Any personal files saved to a user's local computer drive are the sole responsibility of the user and the CSI Pacific IT team shall not be responsible for their backup or recovery. Users must be aware that the IT team can potentially access those files while servicing the computer equipment, therefore they must acknowledge the privacy for those documents will be relinquished the moment they are stored in a corporate device. Saving personal media content on corporate devices for personal entertainment will be allowed if the following conditions are met:

1. Staff productivity is not reduced;
2. Such files are for personal use (not for business purposes);
3. The user has the proper ownership and proper right to use that content for personal use (not illegally downloaded) abiding to all copyright laws;
4. Does not impact the computer equipment performance; and
5. The user acknowledges that CSI Pacific will not take responsibility over such media data (including backing up, migrating, etc) and the ownership will remain with the user.

Incidental personal uses of the Internet, computer equipment and e-mail resources are permissible. Staff is responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or e-mail resources must adhere to the following limitations:

1. It must not cause any additional expense to CSI Pacific;
2. It must not have any negative impact on the staff member's overall productivity;
3. It must not interfere with the normal operation of the staff member's work location (such as increasing the network bandwidth, which could affect the general productivity of the site);
4. It must not compromise the staff member's work location or CSI Pacific in any way; and
5. It must be ethical and responsible.

2. E-MAILS AS CORPORATE RECORDS

E-mail messages, including any electronic attachments, created, collected, received or transmitted in the normal course of business which reflect the functions, business activities, and decisions of the business are corporate records. A record held elsewhere on behalf of CSI Pacific is also under its control (such as at a staff member's home or on business travel). Since most e-mail messages are records, these must be kept. As such, e-mails must not be automatically forwarded to other mailboxes (i.e. personal mailboxes such as Gmail, Hotmail, etc.). Further, it is expected that staff will use their CSI Pacific e-mail account for

all electronic correspondence and will refrain from using personal email accounts for business correspondence.

3. STAFF/USER RESPONSIBILITIES

- Read, acknowledge and sign an acceptable use policy statement before using these resources.
- Use access to the network, Internet and e-mail in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulation.
- As with other forms of publication, copyright restrictions/regulations must be observed.
- Staff shall be aware that their conduct or information they publish could reflect on the reputation of CSI Pacific. Therefore, professionalism in all communications is of the utmost importance.
- Staff that choose to use e-mail to transmit sensitive or confidential information should encrypt such communication using approved products for secure electronic messaging services.
- Staff shall represent themselves, CSI Pacific accurately and honestly through electronic information or service content.

4. LEAD RESPONSIBILITIES

- Leads are required to identify network, computer equipment and e-mail training needs and resources, to encourage use of network and e-mail resources to improve job performance, to support staff attendance at training sessions, and to permit use of official time for maintaining skills, as appropriate.
- Leads are expected to work with staff to determine the appropriateness of using the network, computer equipment and e-mail resources for professional activities and career development, while ensuring that staff does not violate the general provisions of this policy, which prohibit using network and e-mail resources for personal gain.
- Leads who suspect that an employee is using e-mail inappropriately must advise senior management in writing before attempting to gain access to the staff member's e-mail account.

5. PROHIBITED AND UNACCEPTABLE USES AND CONSEQUENCES

Use of network, computer equipment and e-mail resources is a privilege that may be revoked at any time for unacceptable use or inappropriate conduct. Any abuse of the acceptable use policies may result in notification of the Institute's management, revocation of access and disciplinary action up to and including dismissal. The following activities are, in general**, strictly prohibited**. With the proper approval, staff may be exempt from certain prohibitions during the course of job responsibilities and legitimate CSI Pacific business.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including but not limited to, the downloading, installation or distribution of pirated software, digital music and video files.
- Engaging in illegal activities or using the Internet or e-mail for any illegal purposes, including initiating or receiving communications that violate any provincial, federal or local laws and regulations. This includes malicious use, spreading of viruses, and hacking. Hacking means gaining or attempting to gain the unauthorized access to any computers, computer networks, databases, data or electronically stored information.
- Using network and e-mail resources for personal business activities in a commercial manner such as buying or selling of commodities or services with a profit motive.
- Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency or size of messages. This includes statements, language, images, e-mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

- Using abusive or objectionable language in either public or private messages.
- Knowingly accessing pornographic sites on the Internet and disseminating, soliciting or storing sexually oriented messages or images.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or e-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of e-mail.
- Staff is not permitted to use the e-mail account of another employee without receiving written authorization or delegated permission to do so.
- Staff is not permitted to forge e-mail headers to make it appear as though an e-mail came from someone else.
- Sending or forwarding chain letters or other pyramid schemes of any type.
- Sending or forwarding unsolicited commercial e-mail (spam) including jokes.
- Soliciting money for religious or political causes, advocating religious or political opinions and endorsing political candidates.
- Making fraudulent offers of products, items, or services originating from any CSI Pacific account.
- Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy or where such distribution is contrary to the CSI Pacific Privacy Policy.
- Online investing, stock trading and auction services such as eBay unless the activity is for CSI Pacific business.
- Developing or maintaining a personal web page on or from a CSI Pacific device.
- Use of peer-to-peer (referred to as P2P) networks such as Bit Torrent, Kazaa, Gnutella, Grokster, Limewire and similar services.
- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to: Internet games, online gaming, unnecessary Listserve subscriptions and E-mail attachments, chat rooms and messaging services such as Internet Relay Chat (IRC), I SeeK You (ICQ), AOL Instant Messenger, MSN Messenger and similar Internet-based collaborative services. Skype may be employed provided that it is used for business only and that all steps have been taken by users to protect the host computers from viruses, trojans and similar such malicious software.
- Streaming music and video from Internet sites while connected to a corporate network during regular business hours, except where it is required to carry out job duties, as these types of activities cause network congestion and affect overall network performance, compromising access to corporate resources such as shared drives. Streaming in any other circumstances is allowed as long as it does not interfere with staff's performance of duties.
- Installing software that has not been approved by the IT team and which does not relate to the user's role at CSI Pacific, since it could potentially affect the overall performance of the corporate data or be an actual virus or malware.
- Connecting, or permitting the connection of, a non-CSI Pacific computer or computing device to the CSI Pacific business network without the previous authorization of the IT Department (which will perform a series of actions to confirm the device complies with the corporate security standards). This includes equipment belonging to our partners and clients.

PASSPHRASE POLICY

Approved September 19, 2014

POLICY STATEMENT

Passphrases are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen passphrase may result in the compromise of CSI Pacific's entire corporate network. As such, all CSI Pacific employees (including contractors and vendors with access to CSI Pacific systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passphrases.

DEFINITIONS

The following terms have these meanings in this Policy:

a) "*Passphrase*" – A concept that replaces the more traditional "password". The main and basic difference is that you can use **multiple words and characters, including spaces and tabs, when creating** a passphrase. This results in a *more secure and hard to break authentication* method making a dictionary-based attack quite difficult.

APPLICATION

The passphrase policy will establish a standard for creation of strong passphrases, the protection of those passphrases, and the frequency of change.

This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a passphrase) on any system that resides at any CSI Pacific facility, has access to the CSI Pacific network, or stores any non-public CSI Pacific information.

PROCEDURES

1. GENERAL

- All system-level passphrases (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least in a quarterly basis.
- All user-level passphrases (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique passphrase from all other accounts held by that user.
- Passphrases must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passphrases must conform to the guidelines described below.

2. GUIDELINES

Passphrases are used for various purposes at CSI Pacific. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. Since none of our systems have support for one-time tokens (i.e., dynamic passphrases which are only used once), everyone should be aware of how to select strong passphrases.

Poor, weak passphrases have the following characteristics:

- The passphrase contains less than fifteen characters;
- The passphrase doesn't make use of any complexity characteristics, such as:
    - Upper and lower case characters;

- Digits and / or punctuation characters;
- Purposely misspelled words; and

- The passphrase is based on organization, family names or other personal references. “canadiansportinstitutepacific” would make a poor passphrase as would “johnsmithspassphrase”.

Strong passphrases have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Are at least fifteen alphanumeric characters long (can be as long as 128 characters);
- Are not based on personal information, names of family, etc.; and
- Passphrases should never be written down or stored on-line. Try to create passphrases that can be easily remembered. One way to do this is create a passphrase based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the passphrase could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use any of these examples as passphrases!

3. PASSPHRASE PROTECTION STANDARDS

Do not use the same passphrase for CSI Pacific accounts as for other non-CSI Pacific access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same passphrase for various CSI Pacific access needs. For example, select one passphrase for the email systems and a separate passphrase for desktop computer systems.

Do not share CSI Pacific passphrases with anyone, including athletes, coaches or volunteers. All passphrases are to be treated as sensitive, confidential CSI Pacific information.

Here is a list of "don’ts":

- Don't reveal a passphrase over the phone to ANYONE;
- Don't reveal a passphrase in an email message;
- Don't reveal a passphrase to the boss;
- Don't talk about a passphrase in front of others;
- Don't hint at the format of a passphrase (e.g., "my family name");
- Don't reveal a passphrase on questionnaires or security forms;
- Don't share a passphrase with family members; and
- Don't reveal a passphrase to co-workers while on vacation.

Do not use your assigned user name / passphrase to log someone else into the CSI Pacific computer networks or web-based applications. Such action severely compromises the security of the networks and your personal account and may be considered grounds for dismissal.

If someone demands a passphrase, refer them to this document or have them call someone in the Information Technology Department.

Do not use the "Remember Password" feature of applications (e.g. Outlook, Internet Explorer).

Again, do not write passphrases down and store them anywhere in your office. Do not store passphrases in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passphrases at least once every six months (except system-level passphrases which must be changed quarterly). The recommended change interval is every four months.

If an account or passphrase is suspected to have been compromised, report the incident to Information Technology and change all passphrases.

Passphrase cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a passphrase is guessed or cracked during one of these scans, the user will be required to change it.

4. USE OF PASSPHRASES FOR REMOTE ACCESS USERS

Access to the CSI Pacific networks via remote access is to be controlled using either a one-time passphrase authentication or a public/private key system with a strong passphrase.

5. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action.