Information Security - General

Approved by: Vice President, Corporate Security & Compliance
Last Reviewed: December 2013

Purpose

The purpose of this policy is to provide direction as to the acceptable uses of BCLC's information and systems from a security standpoint, including but not limited to: making certain that BCLC employees and contractors have the direction and knowledge required to adequately protect BCLC's information assets from unauthorized access, use or disclosure; safeguarding the personal information contained within BCLC's systems; fulfilling BCLC's obligations to conduct and manage gambling within B.C. in accordance with the *Gaming Control Act*, the *Freedom of Information and Protection of Privacy Act* (FIPPA) and other applicable standards and legislation; and protecting BCLC's reputation.

SCOPE

This policy applies to the use of all BCLC computing resources or equipment that is owned or leased by BCLC and applies regardless of the physical location of the user or the system.

This document is part of the BCLC Information Privacy and Security Policy and Compliance Framework.

POLICY STATEMENT

Effective privacy and security require the integration of people, policy and technology. This policy provides the security requirements for information protection throughout BCLC, including requirements for maintaining user access and authorizations for BCLC computer networks, operating systems, databases, applications and information.

POLICY DETAILS

1.0 General Requirements

Access to and use of computing resources at BCLC is provided to assist in the delivery of BCLC services and generation of revenue. All use of computing resources including, but not limited to, the Internet and e-mail must comply with the requirements set out in this policy.

FIPPA directs how BCLC may collect, access, use, store, disclose and dispose of Personal Information. FIPPA requirements are included in BCLC's Privacy Policy and all users of BCLC's computing resources must comply with BCLC's Privacy Policy and Privacy Breach Policy.

2.0 Personal Use

In recognition of the need most users have to take care of occasional personal matters during breaks and non-working hours, reasonable personal use of computing resources is allowed, provided that it does not interfere with BCLC's operations or incur additional cost to BCLC.

Information Security - General

Personal use must comply with all of the requirements laid out in this policy. BCLC will not change system settings, such as those on the firewall or the Internet content filter, to accommodate personal use.

The use of social media must be in accordance with BCLC's Use of Social Media guidelines.

3.0 Ownership of Information and Access to Technology Records

Users must be aware that all computing activities generate records of use including the date, time and type of access. These records are generated regardless of whether the usage is business or personal. Systems that log and monitor usage do not differentiate between business use and personal use.

All information stored or recorded on or through BCLC's computing resources, including information marked private, personal and/or confidential, belongs to BCLC and may be accessed by BCLC for regular business, security or audit purposes without notice to the user. Users should not assume an expectation of privacy for any information, including non-work -related information that is viewed, stored or transmitted using BCLC's computing resources.

All messages created, sent or received over the Internet are the property of BCLC and may be regarded as public information. This information may have to be publicly released if requested under FIPPA. In addition, all communications can be disclosed to law enforcement or other third parties as permitted or required by law without prior notification to the individuals involved.

The Vice-President, Corporate Security and Compliance, Director Information Privacy and Security, or designate may access a user's technology usage records or e-mail at any time without notice to the user to support a security or compliance review or investigation.

The Information Privacy and Security team will co-ordinate the collection and/or disclosure of any user access records and will accept internal requests only from an employee's direct Manager (or a higher level of management).

4.0 Acceptable Use

BCLC is committed to maintaining a respectful workplace environment. The Harassment Policy details behaviours that are considered to be harassment and how harassment will be investigated and dealt with. Use of BCLC's computing resources must not contravene this or any other BCLC policies.

Users are representing BCLC and are responsible for making certain that the Internet is used in an effective, ethical, and lawful manner.

5.0 Internet Use

The Internet is openly accessible to the public. Information transmitted on the Internet or stored on servers accessible via the Internet is insecure and may be logged or viewed by unintended audiences.

Activities on the Internet can be traced to the address from which they originate and therefore Internet usage must be able to survive public scrutiny or disclosure.

Users must not knowingly attempt to access websites that might bring BCLC into disrepute, such as those that contain material that violates any of BCLC's policies or those that contain pornography, hate literature,

Information Security - General

or any material that contravenes the B.C. Human Rights Code, Criminal Code or any other federal or provincial law.

In the event that a user accidentally encounters a website containing content as noted above, the website must be closed immediately and no further actions taken on the site.

BCLC employs an Internet content filter to restrict access to Internet sites that fall into certain categories. This system is configured to block access to websites that have been categorized as containing inappropriate content. The following criteria are used by BCLC to determine if a website should be blocked:

1. Sites that are clearly inappropriate for the business functions of BCLC;
2. Sites that are potentially socially/morally offensive and do not support the operating principles and practices of BCLC;
3. Sites that may expose BCLC to legal liability; and/or,
4. Sites with a strong potential for a security breach.

Based on the above criteria, BCLC may block Internet access to specific sites.

Using file sharing programs, operating or supporting outside business interests using BCLC resources or transmitting any content that is offensive, harassing, or fraudulent are unacceptable uses of BCLC's computing resources.

Departmental Internet connections that operate outside of BCLC's standard Internet access are generally not permitted. If there is a valid business requirement for a separate Internet connection, it must be assessed based on risk and approved by both Business Technology and the Information Privacy and Security team prior to implementation.

6.0 Voicemail, Email and Instant Messaging Use

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Users should be aware that voicemail will be automatically sent to email as an audio file. Voicemail and email messages that are not required to be retained as business records are considered transitory and should be deleted when no longer needed.

Text or instant messages, such as those sent via a mobile device or instant messaging program, are considered transitory records and as such are not retained on, or backed up from, any BCLC systems. Users have the ability to copy and save or send the contents of instant messages. Text or instant messaging should not be used where a business record of the communication is required to be retained.

Blanket forwarding of messages to parties outside of BCLC, including automatic forwarding to a non-BCLC Internet email address, is prohibited.

Users must refrain from sending or forwarding chain e-mail or broadcasting email to more than 10 recipients or more than one distribution list, unless directly related to BCLC business.

Information Security - General

7.0 Malware

Malware is software that is intended to damage or disable computers and computer systems. Malware can cause destruction of corporate resources and is much easier to prevent than to recover from. Defences against malware include protection against unauthorized access to computer systems, using only trusted sources of data and programs, and maintaining virus-scanning software.

Where possible and practicable, all corporate-owned, -leased, or -operated workstations and servers must have BCLC's standard antivirus software installed, running and maintained with current definition files. All signature files and engine versions must also be kept current.

Antivirus software must not be deactivated on any system, including a workstation, without permission from Information Privacy and Security.

Users must not knowingly introduce malware into company computers and must not load any portable media of unknown origin, including CDs, DVDs, or USB memory devices.

All incoming CDs, DVDs, USB memory devices and other portable media must be scanned for malware before the files that they contain are opened. Workstation anti-virus software must be configured to automatically scan all files being opened or copied onto the workstation.

Any user who suspects that his/her BCLC laptop or workstation has been infected by malware must immediately power off the computer or disconnect the network cable from the computer and contact the Service Desk.

8.0 Downloads

Downloads of software, movies or music from the Internet are not permitted unless directly related to the user's job function. In the case of software downloads, approval must be obtained from the Service Desk prior to downloading and installing.

Users must respect the legal protection that is provided by:

- Copyright law for computer programs and data compilations, literary, dramatic, artistic or musical works;
- Patent law for inventions;
- Trademark law for names, marks, logos and other representations that serve to distinguish goods or services that are proprietary to an individual or business entity.

9.0 Storage

Storage space on the file servers is limited and therefore users should not store personal files such as photographs, movies or music on BCLC's servers.

All files and information must be securely deleted from any hard drives or removable media that is being transferred to a new user or disposed of. Secure deletion involves overwriting the data three times with random data. Requests for data deletion must be submitted through the Service Desk.

Information Security - General

Sensitive information (including personal information) should be encrypted in transit and at rest to prevent unauthorized access. This includes information stored within BCLC's systems and on laptops, mobile devices and portable storage media such as USB drives. For information on encryption and the options available, users should contact the Service Desk.

10.0 Access Codes and Passwords

Each user is responsible for the security of his/her passwords. Users must not disclose passwords to others and must immediately change passwords if it is suspected that they have become known to others. Users must not use access codes or passwords assigned to other users.

Users must not use system-generated or manufacturer-supplied passwords for anything other than an initial password or first-time sign-on. Manufacturer and application default passwords must be changed prior to a system being implemented for use.

Laptop computers and handheld devices, including Blackberries, iPhones, iPads and other mobile devices, which are used for BCLC business, must be protected with a power-on or encryption password to prevent unauthorized access to the information on the device. For information on how to establish a power-on or encryption password, users should contact the Service Desk.

11.0 Approval, Creation, Change and Removal of Accounts

For each system, an account creation, change and deletion procedure must be in place. This procedure must identify the responsibilities for approving the addition, changes to, or deletion of a user account and the processes to be followed for each. The procedure must also set out the timelines and priority for the deletion of accounts when users leave the organization or transition into new roles.

Accounts permitting any kind of physical access or remote computer access to BCLC systems must be decommissioned as soon as possible and within one business day of the change or termination taking place. Where possible, accounts for network systems or financial systems must also be decommissioned within one business day of the change or termination taking place.

For all other systems, the Business Owner must determine and document the time frame for the decommissioning of accounts based on the level of risk to the system and to BCLC assets.

Where possible, accounts for contractors or fixed-term employees must be configured to automatically lock or disable themselves on the day that the contract or employment agreement ends.

Whenever possible, accounts must be set to auto-disable after a period of inactivity.

Access to BCLC computing resources is provided at the sole discretion of BCLC and may be revoked or suspended in the event of policy violation or inappropriate activity.

12.0 Reviews of Access Rights

Access rights for critical systems, systems that contain personal or confidential information and systems that permit access from outside of BCLC's networks must be reviewed at least annually by the Business Owner responsible for the system to make certain that the permissions assigned to the user accounts remain

Information Security - General

appropriate and that users who no longer require access to the system have been removed. These reviews must include all user accounts within the system, including privileged accounts.

Review should also be completed prior to the introduction of new systems, applications or other services or major technology changes and following any organizational changes or restructuring.

13.0 Least Privilege

Whenever possible, access controls must be maintained based on the principle of least privilege, which requires that any user of a system, including users responsible for administering systems, must be able to access only the information and resources that are necessary to perform authorized tasks.

If any user or account requires any temporary elevation in account privilege, such changes must be documented to make certain that:

- an adequate audit trail exists;
- the request is properly authorized in advance; and
- the elevated access is lowered after the predefined time period.

14.0 Segregation of Duties

Controls must exist to segregate the duties of development, test, authorization and implementation of changes to production environments to reduce the risk of unauthorized use of or changes to corporate assets. Business Owners are responsible for making certain that adequate segregation of duties exists within the systems that they are responsible for.

15.0 Contractor Computers

In situations where there is a requirement for a contractor to plug his/her computer into BCLC's network, the contractor must contact the Service Desk prior to connecting any equipment to BCLC's networks. Any non-BCLC computer must have the most current security patches installed as well as anti-virus with current definitions, anti-spyware and a firewall. These requirements are in place to protect BCLC from malware or compromised computers entering the network.

16.0 Wireless Communications

Wireless technology has no physical boundaries and therefore security is easily compromised and is a significant concern. Users must not install wireless access points on BCLC computing equipment or within BCLC's premises. Business Technology is responsible for the installation and configuration of all wireless equipment. Approval must be obtained from Business Technology prior to any equipment being purchased.

For laptop computers, wireless connections may be enabled provided that the desktop firewall and security software have been configured by the Service Desk and are operational.

The ability to act as a hotspot and provide wireless service must be disabled on all workstations and laptops.

Information Security - General

17.0 Bypassing or Breaching Security Measures

Security measures, such as a firewall, access controls and intrusion detection systems, have been put in place to protect BCLC from breaches that originate from outside sources. Any activity that bypasses or is intended to bypass or disable the security measures that are in place to protect BCLC's networks contravenes this policy.

18.0 Physical Security

It is BCLC's policy to protect computer hardware, software, data and information from misuse, theft, unauthorized access, and environmental hazards. All computing resources should be protected according to the criticality and sensitivity of the system and information stored within it.

Provisions should be made to restrict physical access to sensitive systems and information and to allow for protection against natural disasters, such as floods, fires or earthquakes.

Removable media such as CDs, DVDs and USB memory devices should be encrypted and stored out of sight when not in use.

Each user is responsible for the security of his or her laptop at all times. This includes but is not limited to situations where a laptop is loaned to a user on a temporary basis and times when the device is in a vehicle or at a residence.

19.0 Storage of Cardholder Data Prohibited

BCLC is a merchant that processes credit card payments, therefore, BCLC must comply with Payment Card Industry (PCI) requirements.

To comply with current PCI requirements, the storage of cardholder data in any form (hard copy or electronic) by BCLC is prohibited.

Cardholder data is defined as the full magnetic stripe or the Primary Account Number plus any of the following:

- Cardholder name
- Expiration date
- Service Code

The Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account.

20. 0 Remote Access

Remote access facilities are provided at the discretion of BCLC via BCLC's standard remote access solutions to assist in business operations and the delivery of services. Use of BCLC's remote access facilities must not contravene BCLC's policies.

Non-standard remote access to BCLC's networks is not permitted. Only remote access software approved by Information Privacy and Security and provided by Business Technology may be used to connect to BCLC.

Information Security - General

21.0 Remote Computers

Users who are granted remote access privileges must be aware that once connected to BCLC's network a remote computer becomes an extension of that network and provides a potential point of entry for viruses and hackers. Therefore, users must take all precautions to protect the remote computer from compromise at all times.

To reduce the risk of unauthorized use of BCLC's resources through the compromise of a remote computer, each user who is granted remote access privileges is responsible for making sure that any computer that he/she will use to connect to BCLC has the most current security patches installed as well as anti-virus with current definitions, anti-spyware and a firewall.

22.0 Policy Exemptions

If there is a valid business reason for a user, a software installation, a configuration or a process to operate in contravention of this policy, a request can be made to the Information Privacy and Security team for an exemption. The request must be submitted through the Service Desk and must include the section of the policy that the exemption is requested from along with a clear, thorough explanation of the need for the exemption and the compensating controls in place to reduce the risks associated with policy non-compliance. The Information Privacy and Security team will either approve or deny the request and in the case of an approval, will specify a time frame for the exemption. Permanent exemptions will not be granted.

23.0 Privacy and Security Incidents

Privacy and security incidents must be reported as soon as possible to the Information Privacy and Security team. This includes any incident or suspected incident of malicious or illegal activity involving any corporate information or computing resource.

Information Privacy and Security is responsible for overseeing any security incident response and investigation.

Controls and logging must be in place to log and monitor access to network and information assets to detect unauthorized access or malicious activity. The Information Privacy and Security team is responsible for reviewing these logs on a regular basis to identify privacy and security incidents, including those relating to policy non-compliance.

24.0 Information Privacy and Security Assessment

All new systems and infrastructure components being developed acquired or integrated into BCLC's infrastructure or business processes, including outsourced systems, must be reviewed by Information Privacy and Security to make certain that they meet BCLC's information privacy and security standards and do not adversely impact the security of BCLC's systems, infrastructure or information.

Systems and infrastructure components undergoing significant changes must also be reviewed by the Information Privacy and Security team to make certain that the changes do not adversely impact the security of BCLC's systems, infrastructure or information.

Information Security - General

Requests for information privacy and security assessments must be submitted through BCLC's Service Desk to make certain that they are recorded and prioritized accordingly. The time frame for the assessment will depend on the scope and complexity of the system being assessed. To ensure a timely review and to prevent last-minute changes impacting implementation deadlines, the Information Privacy and Security assessment should be initiated at the commencement of the project or during the planning stages for an implementation or upgrade.

ROLES AND RESPONSIBILITIES

Employees are responsible for:

- Adhering to this policy and all related policies, standards and guidelines
- Asking a manager or member of the Information Privacy and Security team when unsure of how to comply with this policy
- Reporting security alerts, warnings or similar messages to the Information Privacy and Security team
- Reporting any loss or theft of technology products to the Service Desk

Managers are responsible for:

- Making certain that this policy is supported within their business areas
- Making certain that all personnel, including employees, contractors and temporary personnel, are aware of and understand this policy
- Notifying Human Resources in the event that an employee's role changes so that Human Resources can initiate notifications to other parties who may need to review or revise access permissions
- Initiating account closure procedures when an employee or contractor ceases working with BCLC

Information Privacy and Security is responsible for:

- Maintaining this policy
- Making training available to support this policy
- Providing advice and guidance to business units and Business Technology on how to implement systems in compliance with this policy and other security requirements as determined by Information Privacy and Security
- Working collaboratively with Business Technology to develop procedures and standards relating to information privacy and security
- Initiating access rights reviews and notifying the Business Owners and Technical Owners when the reviews should take place

COMPLIANCE

Violations of this policy will be managed in accordance with the Progressive Discipline Policy.

Information Security - General

RELATED MATERIAL

Information Privacy and Security Standards

Information Technology Policies

Privacy Policy

Privacy Breach Policy

Information Privacy and Security Assessment Procedure

POLICY OWNERSHIP

Contact Position	Manager FOI Privacy & Information Governance
Policy Owner Position	Director, Information Privacy & Security
Approving Body	Vice President, Corporate Security & Compliance

REVISION HISTORY

Version Number	Approval Date	Approved by	Amendment
1.2	Jan 29, 2015	Vice President, Corporate Security and Compliance	Minor amendment to footer text. This document was re-classified from 'Internal' to 'Public' in order to comply with a directive from the Public Sector Employers' Council. An exemption to policy approval requirements was made due to exceptional circumstances.
1.1	Dec 18, 2013	Director, Information Privacy & Security	Added a new section "19.0 Storage of Cardholder Data Prohibited" and changed subsequent numbering
1.0	Aug 19, 2013	Vice President, Corporate Security & Compliance	New policy replacing multiple policy documents (guidelines and regulations) related to Information Systems Security