Appropriate Use of Information and Information Technology Resources

Approved by: Vice President, Legal, Compliance, Security
Last Reviewed: April 2018

Purpose

This policy establishes direction on the appropriate use of BCLC Information and Information Technology (IT) Resources to protect BCLC Information from unauthorized access, use or disclosure.

SCOPE

This policy applies to all BCLC employees and Contractors.

This policy applies to the access and use of:

- any IT Resources owned or leased by BCLC, regardless of the physical location of a User or an IT Resource;
- any Device provisioned by BCLC; and
- information in BCLC's Custody or under BCLC's Control.

CONTEXT

The protection of BCLC's Information includes practising safe computing behaviours to reduce the overall occurrence of theft, loss or misuse of BCLC's Information. An Information Security Incident can have serious consequences, including:

- Unauthorized Disclosure of confidential or Personal Information;
- Interruption in BCLC's ability to deliver services;
- Financial losses related to correcting the situation;
- Threats to the safety, health and wellbeing of individuals;
- Legal actions; and
- Loss of public understanding, trust and support.

The collection, access, use, disclosure and disposal of BCLC Information must be conducted in accordance with applicable laws, including the *Freedom of Information and Protection of Privacy Act*, British Columbia, the *Information Management Act*, British Columbia, and the following BCLC policies:

- Standards of Ethical Business Conduct for BCLC Employees and Contractors;
- Privacy Policy and Privacy Breach Policy;
- Records Management; and

Appropriate Use of Information and Information Technology Resources

- Information Classification.

The Allocation of BCLC-Provisioned Devices policy outlines how BCLC devices and peripheral equipment, services or software are allocated to employees and Contractors, including the provision of standard and non-standard devices and software.

Any defined (capitalized) terms used, but not defined in this policy, have the meaning attributed to them in the Policy Glossary of Terms.

POLICY STATEMENT

Access to and use of BCLC's IT Resources is provided to Users to assist in the delivery of BCLC's services. Access is provided at the sole discretion of BCLC and may be revoked or suspended in the event there is a security risk or in accordance with the Compliance section under this policy.

BCLC Information is owned by BCLC. The collection, access, use, transmission, or disposal of BCLC Information or the use of BCLC's IT Resources for any purpose may be audited, inspected, monitored and/or investigated, without notice to the User to:

- maintain, repair and manage IT Resources;
- meet legal requirements to produce information; and
- for legislative, security and policy compliance purposes.

Allegations of inappropriate access, collection, use, disclosure, or disposal of BCLC Information or inappropriate use of BCLC IT Resources is investigated on a case-by-case basis. Investigations may include, but are not limited to, the search and/or seizure of IT Resources.

POLICY DETAILS

Use of IT Resources

Personal Use

Reasonable personal use of IT Resources is permitted during breaks and non-working hours, provided that it:

- does not interfere with a User's duties and responsibilities or BCLC's operations;
- is lawful;
- is not for personal gain; and
- does not compromise BCLC's security or IT Resources or contravene other requirements as laid out in this policy.

Appropriate Use of Information and Information Technology Resources

System settings, such as firewall or internet content filters, will not be changed to accommodate personal use.

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

Use of personal (non-BCLC) email services for BCLC business purposes is not permitted.

Downloads of software, movies or music from the internet are not permitted unless directly related to the User's job function, including audio or video broadcasts of a continuous nature.

Personal files such as photographs, movies or music are not permitted to be stored on BCLC's servers or workstations.

Limited personal files such as photographs, movies or music may be stored on BCLC-provisioned mobile devices. BCLC will not be responsible for maintaining those files. Personal files may be accessed or deleted without notice by the Organizational Unit responsible for cyber security.

Internet Use

Users must use the internet in an effective, ethical, and lawful manner when accessing it through BCLC's IT Resources or Devices or when using the internet to conduct BCLC business.

BCLC employs internet content filters to restrict access to internet sites that fall into certain categories, including websites that have been categorized as containing inappropriate content. The following types of websites are restricted through the use of filters:

- sites that are inappropriate for the business functions of BCLC;
- sites that are potentially offensive, that may contain content that is not appropriate to a respectful and harassment free work environment, or that do not support the operating principles and practices of BCLC; or
- compromised sites that may steal information and/or deliver malware to BCLC IT Resources.

In the event that a User inadvertently encounters a website that has not been filtered and contains any of the above-noted criteria, the User must close the website immediately and take no further actions on the site.

Users are encouraged to use the internet when it is appropriate for business purposes. Users should avoid unnecessary internet use as it causes network and server congestion, incurs additional costs, and puts BCLC's IT Resources at risk.

Appropriate Use of Information and Information Technology Resources

Email, Voicemail and Instant Messaging

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, caution should be exercised when forwarding messages, including email, voicemail, and instant messages.

Users should be aware that voicemail is automatically sent to email and stored as an audio file on their local system.

Blanket forwarding of messages to parties outside of BCLC, including automatic forwarding to a non-BCLC email address, is prohibited. Users must refrain from sending or forwarding chain email or broadcasting email to more than 10 recipients or more than one distribution list, unless directly related to BCLC business.

Information classified as confidential must not be sent using instant messaging tools.

Web Conferencing

Web conferencing sessions, such as those conducted via WebEx, must be supervised by a BCLC employee when a Contractor or third party is providing remote support for BCLC Systems. The supervising employee is accountable for the actions of the remote Contractor.

Utilizing Software (Mobile Applications)

Software, including mobile applications, may only be installed on a BCLC Device in accordance with the Allocation of BCLC Provisioned Devices policy.

Software, including mobile applications, installed on a BCLC Device may have access to Confidential information. When granting software permissions, Users must read the software prompts carefully and only allow permissions that are required. It is the User's responsibility to ensure that no Confidential information is being shared with software that should not have access to this information.

Voice and Data Usage

Where BCLC funds a voice or data access plan, the User must avoid excessive use where possible. The Service Desk Manager will follow up with the appropriate Director on any monthly charges greater than $200. The employee's Organizational Unit may be responsible for reimbursing BCLC for excessive costs.

Appropriate Use of Information and Information Technology Resources

Prohibited Use

The following is a non-exhaustive list of prohibited uses of BCLC's IT Resources:

- Installing personal, unlicensed or pirated software, hacking tools or file-sharing programs without prior assessment and approval;
- Modifying the operating system of any Device;
- Operating or supporting outside business interests using BCLC IT Resources;
- Using BCLC's IT Resources unlawfully, including viewing, receiving or transmitting offensive, harassing, or illegal material, such as material that violates BCLC's policies or that contains pornography, hate literature, or any material that contravenes the B.C. Human Rights Code, Criminal Code, or any other federal or provincial law;
- Installing wireless access points on IT Resources or within BCLC's premises;
- Enabling hotspot functionality on a Device (the ability to act as a hotspot and provide wireless service must be disabled on all Devices);
- Exploiting system vulnerabilities to gain unauthorized access to systems and information without the express consent of the Organizational Unit responsible for cyber security; and
- Any activity that bypasses or is intended to bypass or disable security measures, such as firewalls, internet proxies, endpoint security software, access controls and intrusion detection systems that are in place to protect BCLC's networks from breaches that originate from outside sources.

User Responsibilities

Unattended IT Resources

Each User is responsible for the physical security of all IT Resources within their possession, including when not on BCLC premises. This includes but is not limited to situations where Devices, such as a Portable Storage Device (PSD), are in a vehicle or at a User's residence. Devices must be stored in a safe location and out of sight when not in use. The loss or theft of any IT Resource must be reported immediately to Organizational Unit responsible for cyber security and Service Desk.

Users of BCLC IT Resources must be aware of and understand their role and obligations in reducing the risks of theft, fraud, or misuse. Users must employ safeguards to protect IT Resources, including:

- Locking or logging-off workstations or laptops when not actively using or monitoring those Devices;
- Whenever possible, ensuring the computer is connected to the network at the end of each day for system updates and patches; and
- Securing PSDs in a locked desk, cabinet, or compartment.

Appropriate Use of Information and Information Technology Resources

Damage to IT Resources

Users are responsible for the care and safe keeping of IT Resources at all times while in their possession. The cost of repairing or replacing an IT Resource may be charged to an employee's Organizational Unit where there is damage exceeding normal wear and tear or resulting from misuse not covered under a warranty. Damage to any IT Resource must be reported to Service Desk.

Shared Accounts

All Users must be uniquely identifiable on BCLC platforms and systems. The use of generic or shared accounts is expressly prohibited without the express consent of the Organizational Unit responsible for cyber security.

Accounts created and used for BCLC work purposes must be established using a BCLC-issued email address, where applicable. This applies to BCLC-provisioned mobile devices and third-party cloud or online services.

Access Codes and Passwords

Each User is responsible for the security of their passwords. Users must not divulge, share or compromise their own, or another User's, passwords or user identification, including with individuals responsible for providing technical support. Passwords must be immediately changed if compromise is suspected and the incident reported in accordance with the Information Security Incident reporting requirements below. Users must not use access codes or passwords assigned to other Users.

Default, vendor supplied, or generic passwords must be changed after the initial setup of a Device.

Portable Storage Devices that are used for BCLC business must use encryption to prevent unauthorized access to the information on the Device. For information on encryption and the options available, Users should contact the Service Desk.

Malware

Users who are not aware of safe computing practices may inadvertently assist in the transmission of Malware to BCLC's IT Resources. Endpoint security software, including antivirus and anti-Malware software, must not be deactivated on any system, including a workstation, without authorization. In situations where the use of endpoint security software introduces technical issues on systems, the Organizational Unit responsible for cyber security may authorize limited exemptions for a period not exceeding twelve (12) months to allow software vendors to make necessary changes to accommodate the endpoint security software. Exemptions must be requested and reassessed annually.

Appropriate Use of Information and Information Technology Resources

Users must not knowingly introduce Malware into BCLC's IT Resources. Any User who suspects that a BCLC IT Resource has been infected by Malware must immediately report the incident in accordance with the Information Security Incident reporting requirements below. Security alerts, warnings, and other messages must also be reported.

Use of Non-BCLC-provisioned Devices

Only a BCLC-provisioned Device may be connected to a BCLC IT Resource, unless appropriate approval has been obtained to connect a non-BCLC-provisioned Device.

Users must seek approval from Service Desk and the Organizational Unit responsible for cyber security prior to connecting any non-BCLC-provisioned Devices to BCLC's IT Resources. Any non-BCLC-provisioned Devices must have the most current security patches, anti-virus with current definitions, anti-spyware, and a local firewall, if appropriate. These requirements are in place to protect BCLC from Malware and prevent compromised computers from entering the network.

Information Handling

Information classified as confidential must not be downloaded and/or stored to a non-BCLC Device. The storage of Confidential information is not permitted outside of BCLC's networks (e.g., the cloud) without prior assessment and approval from the Organizational Unit responsible for cyber security.

Information classified as confidential should be encrypted in transit and at rest to prevent unauthorized access. This includes information stored within BCLC's IT Resources and on Devices. For information on encryption and the options available, Users should contact the Service Desk. BCLC Information that is temporarily stored on a Device, such as a PSD, must be transferred to a BCLC network as soon as reasonably practicable.

As per the Payment Card Industry Data Security Standard (PCI DSS), the copying, moving, and storage of credit card data onto local hard drives and removable electronic media is prohibited, unless explicitly authorized for a defined business need. Where there is an authorized business need, credit card data must be protected in accordance with all applicable PCI DSS Requirements

Remote Access

Remote access facilities are provided at the discretion of BCLC. Users who are granted remote access privileges must be aware that once connected to BCLC's network, a computer becomes an extension of that network and provides a potential point of entry for viruses and hackers. All reasonable precautions must be taken to protect computers connected remotely from compromise.

Appropriate Use of Information and Information Technology Resources

When using a non-BCLC provisioned computer to connect remotely to BCLC's networks, Users should make certain that the computer has installed the most current security patches, anti-virus with current definitions, anti-spyware and a firewall, if appropriate.

BCLC-provisioned PSDs must be used, when necessary.

When using non-BCLC wireless access points, Users are at risk of exposing personal and BCLC information to compromise. Users should limit the use of public wireless on BCLC Devices where possible. When it is necessary to connect a BCLC laptop to public wireless, Users must select the "Public" option when prompted by Windows to connect to a public wireless network in order to set the appropriate security posture. Users must use the BCLC Virtual Private Network (VPN) application, Cisco AnyConnect to establish a secure connection. Access to and use of Confidential information from public wireless networks is not recommended.

User's Consent to Collect, Use, and Disclose Personal Information

By accepting a BCLC Device, a User consents to the collection, use, access, storage, disclosure and disposal of the User's personal information by BCLC and its Service Providers, both inside and outside of Canada, in accordance with the *Freedom of Information and Protection of Privacy Act*, British Columbia for purposes related to the administration of the account, monitoring Device usage, and investigating lost or stolen Devices. For more information about privacy at BCLC, refer to the Privacy Policy and Privacy Breach Policy on BCLC's intranet (YAK).

Information Security Incident Reporting

All Users must report Information Security Incidents as soon as possible. This includes any non-compliance with BCLC policies governing information security, all types of Information Security Incidents identified within this policy, and any other incident or suspected incident of malicious or illegal activity involving any BCLC Information or IT Resource.

Users who identify a potential Information Security Incident must immediately report it to the Organizational Unit responsible for cyber security. Any of the following methods may be used:

Website:	Submit an Information Security Incident report through ServiceNow
Email:	Send a detailed account of the event to cybersecurity@bclc.com
Telephone:	Call extension 8085 or 250-377-8085
In person:	Speak directly with an employee from the Organizational Unit responsible for cyber security.

Appropriate Use of Information and Information Technology Resources

COMPLIANCE

Managers are responsible for making certain that all Users, including temporary employees, are aware of and understand this policy. Any User who is unsure of how to comply with this policy must ask their manager or the Organizational Unit responsible for cyber security for further clarification.

Failure to comply with this Policy may result in:

- disciplinary action, up to and including termination of employment, administered in accordance with BCLC's Progressive Discipline policy,
- revocation or suspension of use privileges for an indefinite period,
- additional conditions that must be met in order to restore or retain use privileges,
- civil or criminal liability, and/or
- any costs incurred being charged to the appropriate Organizational Unit.

The Organizational Unit responsible for cyber security shall recommend to its Director which of the above responses, excluding disciplinary action, is appropriate in the event of non-compliance with this Policy. The Director shall defer the matter to a User's manager and Human Resources for consideration.

Exemptions

If there is a valid business reason for a User to operate in contravention of this policy, a request for an exemption can be made to the Organizational Unit responsible for cyber security. Exemption requests must be submitted through ServiceNow and include:

- the section of the policy that the exemption is requested for;
- a clear, thorough explanation of the need for the exemption; and
- compensating controls that are in place to reduce the risks associated with policy non-compliance.

Approval of an exemption requires dual sign-off. A manager from the Organizational Unit responsible for cyber security and the manager of the User who submitted the request have authority to approve exemptions. Requests for exemptions that may result in a significant security risk or that the Organizational Unit responsible for cyber security do not otherwise support may be escalated to a higher management level for approval.

In the event an exemption is granted, a time frame for the exemption must be specified. Permanent exemptions are not granted.

Appropriate Use of Information and Information Technology Resources

DEFINITIONS

BCLC Information – means information that is related to BCLC's business in any way.

Control (of information) – means the power or authority to manage the information throughout its life cycle, including restricting, regulating and administering its use or disclosure.

Custody (of information) – means having physical possession of information. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security.

Device – means hardware used to access BCLC Information Technology Resources. Devices include but are not limited to, Personal Computers (PC), laptops, mobile phones, tablets and PSDs.

Information Security Incident – means:

- an event that can affect BCLC's ability to operate by disrupting or threatening service or protection of data and information;
- a technical event such as an attack on BCLC's networks or infrastructure, including phishing, viruses, malware, denial of service or system intrusion;
- a physical event such as theft or loss of proprietary information, social engineering, and lost or stolen assets (such as Devices); or
- exposure of corporate data and information to unauthorized personnel (internal and external).

Information Technology Resources ("IT Resources") – means BCLC-owned information and communications technologies that include but are not limited to information technology systems and related applications, infrastructure, and networks.

Malware – means software that is intended to damage or disable computers and computer systems.

Personal Information – has the meaning ascribed to it in FIPPA and, as at the date of this policy, means recorded information about an identifiable individual other than Contact Information. An individual's name, address, telephone number, age, sex, sexual orientation, marital status, family status and information about the individual's educational, financial, criminal or employment history are all examples of Personal Information. This list is non-exhaustive.

Portable Storage Devices ("PSD") – means electronic media including but not limited to laptop and notebook computers, removable hard drives, USB storage devices (flash drives, jump drives, memory sticks, memory cards, thumb drives, MP3 players, iPods and PDAs), zip drives, CDs, DVDs, tapes and diskettes.

Appropriate Use of Information and Information Technology Resources

User – means persons authorized to access and/or use BCLC IT Resources and Devices, in accordance with BCLC's Allocation of BCLC-provisioned Devices policy where appropriate.

POLICY OWNERSHIP

Contact Position	Manager, responsible for information security
Policy Owner	Director, responsible for cyber security
Approving Body	Vice President, Legal, Compliance, Security

REVISION HISTORY

Version Number	Approval Date	Approved by	Amendment
1.0	Apr 25, 2018	Vice President, Legal, Compliance, Security	Inaugural document. This policy supersedes the former Information Security-General policy (v1.3), which provided policy direction to both users and administrators regarding appropriate use of BCLC Information and IT Resources.