Policy

APPROVED

Appropriate Use of Information and Information Technology Resources

Purpose

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 with respect to the access, use, and disclosure of:

- BCLC owned or leased IT Resources, regardless of the physical location of a User or an IT Resource;
- Devices provisioned by BCLC or permitted access to BCLC IT Resources; and
- BCLC Information.

Policy Statement

BCLC provides Users with access to and use of BCLC Information and IT Resources 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 Organizational Units responsible for cyber security (BCLC Cyber Security) and Legal may audit, inspect, monitor, and investigate the collection, access, use, disclosure, or disposal of BCLC Information or the use of BCLC's IT Resources for any purpose without notice to the User to:

- maintain, repair, and manage IT Resources;
- meet legal requirements to produce and protect 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 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.

All Users must take responsibility for actively protecting BCLC Information and IT Resources. Users must not collect, access, use, disclose, or dispose of BCLC Information unless authorized to do so and where required to perform their duties.

Users must protect BCLC Information classified as confidential (Confidential Information). This includes, but is not limited to:

- only disclosing Confidential Information, particularly Personal Information, to authorized individuals in a secure manner;
- limiting the amount of Confidential Information, particularly Personal Information, that is disclosed through IT Resources such as email, instant messaging, and other collaboration tools;
- physically storing Confidential Information in the User's workspace (e.g., locked drawers or cabinets); and
- protecting Confidential Information when working in a public environment (e.g., ensuring that the information is not viewable or accessible by others).

Context

LEGAL AND POLICY FRAMEWORK

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, and the *Information Management Act*, British Columbia.

This policy supplements the following BCLC corporate policies, which should be read in conjunction where applicable:

- Standards of Ethical Business Conduct for BCLC Employees and Contractors;
- Privacy Management and Accountability Policy;
- Records Management Policy;
- Software, Applications, and Services Policy;
- Software Proposals Procedure;
- Information Classification Policy and Procedure;
- Internal Communications Policy; and
- Use of Social Media Guidelines.

The Allocation of BCLC-Provisioned Devices Policy outlines how certain IT Resources, such as devices and peripheral equipment, are allocated to employees and Contractors, including the provision of standard and non-standard devices.

Policy

APPROVED

Appropriate Use of Information and Information Technology Resources

POLICY OBJECTIVES

Practising safe computing behaviours supports the protection of BCLC Information by reducing the overall occurrence of theft, loss, or misuse of BCLC Information. An Information Security Incident can have serious consequences, including:

- unauthorized disclosure of Confidential Information, including 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.

Policy Details

USE OF IT RESOURCES

Personal Use

Reasonable personal use of IT Resources is permitted during breaks and non-working hours if 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 or other corporate policies.

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

Personal use of IT Resources is subject to the following conditions:

- Use of social media should be in accordance with BCLC's Use of Social Media Guideline.
- Downloads of 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.

- Use of non-BCLC approved Software, such as email services, file sharing, collaboration services, or other Internet-based personal services for BCLC business purposes, is not permitted.
- A User’s BCLC email address must not be attached to personal online accounts or profiles, including use of a BCLC email address to create a personal account/profile or to access services that are unrelated to BCLC business.

Limited personal files may be temporarily stored on a BCLC-provisioned Device; however, BCLC will not be responsible for maintaining or recovering those files. Personal files stored on BCLC Devices may be accessed or deleted without notice to the User by BCLC.

Internet Use

The Internet must be used 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.
- Sites that have been compromised and may steal information and/or deliver Malware to 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.

Generative AI Technology

Generative Artificial Intelligence (AI) technology is any Software capable of creating content such as text, images, videos, or other data. For example, this may include chatbots such as Microsoft’s CoPilot and ChatGPT, and Google’s Gemini (formerly Bard). Only general purpose generative AI technologies that BCLC has approved may be used for business purposes. For certainty, use of generative AI technologies that are not approved Software under BCLC’s Software, Applications, and Services Policy are prohibited, except for reasonable personal use.

Users must not put Personal Information into generative AI technology, including but not limited to names, email addresses, and player data.

Email, Voicemail and Instant Messaging

Use of email, voicemail, and instant messaging tools are subject to the following restrictions:

- Confidential Information must not be sent using instant messaging tools.
- Users must refrain from sending or forwarding chain emails or broadcasting email to more than 10 recipients or more than one distribution list, unless directly related to BCLC business.
- Blanket forwarding of messages to parties outside of BCLC, including automatic forwarding to a non-BCLC email address, is prohibited. Caution should be exercised when forwarding messages, including email, voicemail, and instant messages, as some information is intended for specific individuals and may not be appropriate for general distribution.

Software, Applications, and Services

Software, including cloud-based software services and mobile applications, may only be acquired, installed, or used on a BCLC Device in accordance with the Software, Applications, and Services Policy and Software Proposals Procedure. For guidance, use includes but is not limited to registering an account, inputting information, downloading information, or uploading information to a website.

Software that is acquired, installed, or used on a Device could have access to Confidential Information. When granting Software permissions, Users must read the Software prompts carefully and only allow permissions that are required.

Users must ensure that no Confidential Information is 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.

Portable Storage Devices

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.

Prohibited Use

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

- Installing personal, unlicensed, or pirated software; hacking tools; remote access tools; or file-sharing programs without prior assessment and approval.
- Modifying the operating system of any Device.
- Using IT Resources to operate or support outside business interests.
- Using IT Resources unlawfully or in violation of BCLC's policies, including viewing, receiving, or sharing offensive material, harassing material, pornography, hate literature, or any material that contravenes the *Human Rights Code*, British Columbia, the *Criminal Code*, Canada, or any other federal or provincial law.
- Installing wireless access points on IT Resources or within BCLC's premises.
- Knowingly installing or downloading Malware onto IT Resources.
- Exploiting system vulnerabilities to gain unauthorized access to systems and information without the express consent of BCLC Cyber Security.
- Any activity that bypasses or is intended to bypass or disable security measures, such as firewalls, network security controls, endpoint security software, access controls, and intrusion detection systems that are in place to protect BCLC's IT Resources from breaches that originate from outside sources.

USER RESPONSIBILITIES

Information Handling

Internal and Confidential Information, including Personal Information, must not be downloaded or stored to a non-BCLC-provisioned Device. The upload and storage of internal and Confidential Information is not permitted outside of BCLC's IT Resources (e.g. the cloud) without prior assessment and approval from BCLC Cyber Security. For more guidance on identifying and classifying information, Users should refer to BCLC's Information Classification Policy.

Confidential Information 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 Portable Storage Device, 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 and storage of Cardholder Data to BCLC internal or external servers, local hard drives, and removable electronic media is prohibited, unless explicitly authorized for a defined business need. Where there is an authorized business need, Cardholder Data must be protected in accordance with all applicable PCI DSS Requirements.

Appropriate Use of Information and Information Technology Resources

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, 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 BCLC Cyber Security and the Service Desk.

Users of 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 BCLC network to obtain system updates and patches.
- Securing Portable Storage Devices in a locked desk, cabinet, or compartment.

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 prohibited without the express written consent of BCLC Cyber Security.

Usernames and Passwords

Usernames created and used for BCLC work purposes must be established using a BCLC-issued email addresses. This applies to BCLC-provisioned mobile Devices and third-party cloud or online Software services.

Where Single Sign On (SSO) integration is not supported or feasible, a unique password must be created. Users must not use a current or recent password for non-SSO supported logins.

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 to anyone, including individuals responsible for providing technical support. Users must immediately change their password if they suspect it is compromised and they must report the incident in accordance with the requirements below. Users must not use usernames or passwords assigned to other Users.

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

Malware

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, BCLC Cyber Security may authorize limited exemptions for a period not exceeding 12 months to allow Software vendors to make necessary changes to accommodate the Endpoint Security Software. Exemptions must be requested and reassessed annually.

Any User who suspects that an IT Resource has been infected by Malware must immediately report the incident.

Use of Non-BCLC-provisioned Devices

Only BCLC-provisioned Devices may be connected to IT Resources, except where permitted in this policy. For certainty, Users are prohibited from connecting a non-BCLC provisioned Device, either wirelessly to a secured BCLC network or physically to a network port in a BCLC office, data centre, or facility.

Users are permitted to connect personal devices to BCLC's guest wireless network.

Users must seek approval from Service Desk and BCLC Cyber Security prior to physically connecting any non-BCLC-provisioned Devices to IT Resources.

Remote Access

Remote access capabilities are provided to BCLC Users. Users must be aware that after connecting to BCLC's network, a computer Device becomes an extension of that network and provides a potential point of entry for Malware and unauthorized access.

Users risk exposing BCLC Information to compromise when using non-BCLC networks such as public wireless internet. Users should limit the use of public wireless internet where possible. To establish a secure connection, Users must use one of the following approved methods to connect remotely:

- a cellular network where connecting with a smart phone;
- BCLC's Virtual Private Network (VPN) application, Cisco AnyConnect, where connecting with a Wi-Fi enabled Device, such as laptops or tablets; or
- BCLC's secure access gateway (Citrix) where enforced.

Access to and use of BCLC Confidential Information from public wireless internet is not recommended.

Users must utilize an approved method to connect remotely to BCLC's IT Resources when using a non-BCLC provisioned Device. Users must ensure that their Device has the latest security patches installed and is running appropriate Endpoint Security Software.

A BCLC employee must supervise any support session of a BCLC system where a Vendor conducts the session through remote control access, such as those conducted via Teams or web conferencing services. The supervising employee is accountable for the Vendor's actions during the support session.

USER'S CONSENT TO COLLECT, USE, AND DISCLOSE PERSONAL INFORMATION

By accepting or accessing a BCLC Device or BCLC Software, a User consents to the collection, access, use, disclosure, storage, and disposal of the User's Personal Information by BCLC and its Vendors, both inside and outside of Canada, in accordance with the *Freedom of Information and Protection of Privacy Act*, British Columbia, for purposes related to:

- administration of Devices and Software;
- monitoring Device and Software usage;
- investigating lost or stolen Devices; and
- to comply with applicable law.

For more information about privacy at BCLC, refer to the Privacy Management and Accountability Policy on BCLC's intranet.

INFORMATION SECURITY INCIDENT REPORTING

All Users must immediately report Information Security Incidents. 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 BCLC Cyber Security. Any of the following methods may be used:

Website:	Submit an Information Incident report through ServiceNow
Email:	Send a detailed account of the event to cybersecurity@bclc.com
Telephone:	24/7 – Call 250-377-2085
In person:	Speak directly with an employee from BCLC Cyber Security

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 BCLC Cyber Security for further clarification.

Failure to comply with this Policy may result in:

- disciplinary action, up to and including termination of employment;
- revocation or suspension of use privileges for an indefinite period;
- additional conditions that must be met to restore or retain use privileges;
- civil or criminal liability; or
- any costs incurred or excessive costs being charged to the appropriate Organizational Unit.

BCLC Cyber Security will 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 will defer the matter to a User's manager and People and Culture for consideration.

Appropriate Use of Information and Information Technology Resources

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 BCLC 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 BCLC 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 BCLC Cyber Security does 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

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

Artificial Intelligence (AI)	Has the meaning attributed to it in the Information Security Policy.
BCLC Information	Means information that is related to BCLC's business in any way.
Cardholder Data	Refers to credit card related data such as a credit card number, card verification code (CVC), and related data. The specific nature of this data is defined by the Payment Card Industry Data Security Standard (PCI DSS).
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 Portable Storage Devices.
Endpoint Security Software	Managed software installed on a Device to detect, prevent, and respond to Malware and malicious activities.
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 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	Means electronic media that is easily moved or carried 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), zip drives, CDs, DVDs, tapes and diskettes.
Software	Has the meaning attributed to it in the Software, Applications, and Services Policy.
User	Means BCLC employees or Contractors who are authorized to access and/or use BCLC Information and IT Resources and Devices, in accordance with BCLC's policies and procedures.

Policy Ownership

Contact Position	Director, Cyber Security
Policy Owner	Director, Cyber Security
Approving Body	Vice President, Business Technology

Revision History

Version	Effective	Approved by	Amendment
4.0	Oct 15, 2024	Vice President, Business Technology	Major amendments to add a new section on the use of generative AI technology, and to add, update, strengthen, or clarify directions in almost all sections of the policy.
3.1	Sep 16, 2022	Director, Cyber Security	Minor amendment to update telephone contact information for reporting Information Security Incidents.

Policy

APPROVED

Appropriate Use of Information and Information Technology Resources

Version	Effective	Approved by	Amendment
3.0	Mar 26, 2021	Vice President, Business Technology	Transfer of authority of Policy Owner and Approving Body.
2.3	Mar 19, 2021	Policy Analyst	Correction of typographical error.
2.2	Oct 27, 2020	Chief People Officer	Updates to People and Culture titles to reflect changes following the organizational restructure for OneBCLC.
2.1	Mar 20, 2020	Director, Security, Privacy and Compliance	Amended conditions for personal use of BCLC IT Resources and clarifications to prohibited use of IT Resources.
2.0	Dec 20, 2019	Vice President, Legal, Compliance, Security	New general requirements added to the policy statement to protect BCLC Information and IT Resources. Clarifications throughout the policy, including the scope of the policy, the meaning of confidential information and restrictions on personal use of IT Resources. Revised definition for "User" and new contact information for reporting Information Security Incidents after hours.
1.1	Jun 26, 2019	Vice President, Legal Compliance, Security	Removed reference to the Progressive Discipline Policy.
1.0	Apr 25, 2018	Vice President, Legal, Compliance, Security	Inaugural issue. This policy supersedes the former Information Security - General Policy, which provided policy direction to both users and administrators regarding appropriate use of BCLC Information and IT Resources.