Information Security Standard

Department Responsible: IT Services
Published Date: 2020 June 02

Introduction

BCIT is committed to taking appropriate measures to preserve the confidentiality, integrity, and availability of information and information technology (IT). The Office of the CIO has adopted an Enterprise Architecture (EA) and Cyber Security program which establishes a framework for managing information assets. Both programs are intended to:

- Ensure quality and safety of information;
- Optimize value for money in technology investments;
- Enable business optimization and transformation; and
- Maximize the ability to deal with change.

The adoption of Standards directly supports the achievement of the EA and Cyber Security programs.

Purpose of Standards

The purpose of Standards is to serve as an authoritative and practical compendium of existing and proposed IT architectures and standards. Standards are established norms or requirements that help clarify, guide and control IT processes and activities. They help create a common language with which systems people and business people can communicate about the relationship between business needs and technology solutions.

Information Security Standards are determined by both BCIT and industry, and are published both internally to the community and to vendor partners. Security Standards describe parameters, features, or configurations that define the context-specific requirements. The implementing business unit may choose the appropriate method to satisfy the standard, as long as the security objective of the standard is met or exceeded.

Contents

Introduction	1
Purpose of Standards	1
Who This Policy Applies To	2
Scope	2
Special Situations	2
Standard Details	2
Amendment History	10
Scheduled Review Date	10

Who This Policy Applies To

All owners and managers of BCIT information, BCIT Information Assets and BCIT systems.

Scope

The scope of this document is to provide a working set of general requirements that provide guidance and direction with regards to information security. Its primary focus is on the integrity of the infrastructure and processes required for delivering applications and services throughout the institute.

Special Situations

The BCIT Information Security Standards are reviewed annually, and as required to ensure accuracy and applicability by the Cyber Security Officer (CSO). There will be cases where published standards either do not meet the specific business needs or may be inconsistent with emerging industry standards. The CSO must be consulted well before any procurement or implementation decision is made if BCIT's published security standards may not be appropriate for business needs.

Exceptions from existing published standards will be reviewed by the CSO and further approval and signoff will be required by the CIO.

Standard Details

1. Password and Passphrase Protection
2. Encryption Requirements
3. Secure Application Development
4. Application Security Verification
5. System Hardening
6. Network Segmentation
7. Network Security
8. Internet-Facing Security
9. Logging and Monitoring
10. Account and Sessions Management
11. Privileged Account Management
12. Vulnerability Monitoring and Management

1. Password and Passphrase Protection

Passwords (words or strings of characters) and passphrases (sequences of words or other text) are common and important ways to access and protect digital information on or off the Internet through almost any type of device. Consequently, attackers attempting to access information use a variety of tools to guess or steal passwords/passphrases.

Technical Standard #01

At BCIT, passwords contain a minimum of 8 characters and a passphrase style is recommended instead of a password. Passphrase must include:

- one upper case letter;
- one lower case letter;
- one number; and
- one special character.

Follow top five ways to keep password/passphrase safe:

- create a strong passphrase password; avoid simple/common passwords;
- guard it carefully (e.g. don't share it or write it down);
- do not use BCIT passwords for systems outside of BCIT;
- update password in case of potential threat or compromise; and
- use different passwords for different services.

A secure password vault must be used for storing and sharing passwords. KeePass (http://keepass.info) is a reliable and free open source password manager for individuals. For schools or departments that require a central management and sharing of passwords refer to 1Password (http://1password.com).

2. Encryption Requirements

This section defines BCIT's technical standard that must be used when encrypting devices, files and traffic to safeguard Personal Information and Confidential information. This standard incorporates the legal requirement to encrypt Personal Information stored on a laptop or a mobile Device, which has been affirmed by the British Columbia Information and Privacy Commissioner in interpretation of the *Freedom of Information and Protection of Privacy Act*.

Encryption usage must follow the Encryption Requirements below.

Device	Encryption	Recommended Encryption
Windows Laptop & Desktop	Full disk encryption	Windows BitLocker
Apple Laptop & Desktop	Full disk encryption	Apple FileVault
Mobile Smart Devices	Device-level encryption	MDM or ActiveSync enforced encryption
Media Storage (USB keys, CDs, backup tapes, portable hard drives)	Device/media-level encryption	Microsoft BitLocker to Go, Kingston DataTraveler Vault, IronKey.

Technical Standard #02

Encryption Algorithms	AES-128, AES-192, AES-256
Digital Signature Algorithms	RSA-2048
Cryptographic Hash Ciphers	SHA-2, SHA-3

1. Weak ciphers must be deprecated (e.g. less than 128 bits; no NULL ciphers, 3DES, MD5).
2. Weak protocols must be deprecated (e.g. SSLv2, SSLv3, TLSv1).
3. Secure Renegotiation should be enabled.
4. No Export (EXP) level cipher suites.
5. X.509 certificates key length must be strong (e.g. if RSA key must be at least 2048 bits).
6. X.509 certificates must be signed only with secure hashing algorithms (SHA-2, SHA-3).
7. Keys must be generated with proper entropy (e.g., no weak key generated with Debian).
8. Server should be protected from BEAST Attack.
9. Server should be protected from CRIME attack, TLS compression must be disabled.
10. Server should offer a preferred order of cipher suites, with priority assigned to support Forward Secrecy (e.g. ECDHE suites, followed by DHE suites as a fallback).

3. Secure Application Development

This section defines BCIT's technical standard that software developers must be aware of when working and developing custom applications. BCIT relies on industry best practices and standards, namely NIST and OWASP, when defining the proactive controls and techniques that must be applied proactivity during early stages of software development life cycle.

The list is ordered by importance with item # 1 being the most important:

1. Define Security Requirements
2. Leverage Security Frameworks and Libraries
3. Secure Database Access
4. Encode and Escape Data
5. Validate All Inputs
6. Implement Digital Identity
7. Enforce Access Controls
8. Protect Data Everywhere
9. Implement Security Logging and Monitoring
10. Handle All Errors and Exceptions

Technical Standard #03

At BCIT, all application development must adhere to **OWASP Top 10 Proactive Controls**.

4. Application Security Verification

This section defines BCIT's technical standard when reviewing and verifying BCIT applications especially web enabled applications. All web enabled applications must undergo a security assessment for common web application vulnerabilities such as SQL injection (SQLi), Cross-site

scripting (XSS), HTTP header injection, Directory Traversal, Remote File Inclusion and Command Execution. BCIT relies on industry best practices and standards, namely NIST, CIS and OWASP, when defining the standard.

The list below highlight 14 key verification areas:

1. Architecture, Design and Threat Modeling Requirements
2. Authentication Verification Requirements
3. Session Management Verification Requirements
4. Access Control Verification Requirements
5. Validation, Sanitization and Encoding Verification Requirements
6. Stored Cryptography Verification Requirements
7. Error Handling and Logging Verification Requirements
8. Data Protection Verification Requirements
9. Communications Verification Requirements
10. Malicious Code Verification Requirements
11. Business Logic Verification Requirements
12. File and Resources Verification Requirements
13. API and Web Service Verification Requirements
14. Configuration Verification Requirements

Technical Standard #04

At BCIT, application verification must adhere to **OWASP Application Security Verification (ASVS) Standard 4.0 Level 2.** The ASVS covers off the primary aspects of any sound security architecture: availability, confidentiality, processing integrity, non-repudiation, and privacy.

5. System Hardening

This section defines BCIT's technical standard when implementing system hardening approach to various IT assets (desktops and servers). At BCIT, system hardening takes the fundamental approach of disabling and removing unnecessary features and functionalities in any system. This enables security teams to proactively minimize vulnerabilities, enhance system maintenance, support compliance, and ultimately reduce the system's overall attack surface. BCIT relies on industry best practices and standards, namely NIST and CIS, when identifying and protecting assets as part of system hardening.

Technical Standard #05

At BCIT, system hardening of images must adhere to the **Center of Internet Security (CIS) Benchmarks.** CIS Benchmarks are the global standard and recognized as best practices for securing IT systems and data against the most pervasive attacks.

The list below highlights key configurations requirements when hardening system(s)/image:

1. Systems must be set up in a protected network environment or by a method that assures (local firewall) the system is not accessible via a potentially hostile network until it is secured.

2. Operating system and application services security patches should be installed expediently (e.g. 72 hours) and in a manner consistent with change management procedures.
3. Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.
4. Limit connections to services only to the authorized users of the service.
5. Services or applications running on systems manipulating confidential data should implement encrypted communications as required by confidentiality and integrity needs.
6. If the operating system supports it, integrity checking of critical operating system files should be enabled and tested.
7. Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.
8. The required BCIT institute welcome warning banner should be configured.
9. Apply the principle of least privilege to user, admin, and system accounts. Administrative accounts must not be used as a primary user account or for non-administrative purposes.
10. Enable session timeout of 30 minutes (inactivity) for all accounts.
11. Management IP of a system and service IP (HTTPS) must be separated.
12. Disable IPv6 if not being used.
13. Turn off OS Fingerprint.
14. Disable weak ciphers and configure acceptable order.
15. Enable HTTP Strict Transport Security.

6. Network Segmentation

This section defines BCIT's technical standard when designing and architecting BCIT networks. For effective security, networks must be divided into one or more logical network zones to limit the impact of a network intrusion. Network segmentation is achieved via purpose-built controls that specifically create and enforce separation (zones) and prevent compromise from other zones or networks.

Technical Standard #06

BCIT defined network segmentation must adhere to:

1. Administrative Zone – for devices issued and trusted by BCIT for BCIT's business purpose
2. Student Zone – for student labs owned and maintained by BCIT; BYOD network
3. Research Zone – for research equipment owned by BCIT
4. Residence Zone – for students in their residence
5. Server Zone – for systems connected and accessed internally within BCIT
6. DMZ-External – for systems connected to the internet
7. DMZ-Internal – for backend systems (database servers) serving data to DMZ-External
8. PCI Zone – for systems and devices that handle payment card information
9. Wireless Zone – for wireless users
10. Tenant Zone – external vendors, partners or tenants

The list below highlights key configuration requirements when segmenting networks:

1. Server Zone and DMZ must be configured as private networks using **RFC1918**.
2. All inter-zone traffic must be configured based on filtering (host, service or network).
3. All inter-zone traffic must be over secure channels (SFTP, HTTPS, SSHv2).

7. Network Security

This section defines BCIT's technical standard when securing BCIT network infrastructure. For effective security management, principle of least privilege must be practiced.

Technical Standard #07

BCIT defined network security practices must adhere to:

1. Access to network devices must be controlled by ACL
2. Plain-text protocols must not be used on BCIT networks
3. Management traffic must be separated from user traffic
4. Only secure protocols must be used for network management (e.g. SSHv2)
5. HIDS/NIDS/FIM must be configured and logged
6. DHCP/ARP snooping must be enabled and configured on networks
7. All network connected devices must have their default passwords changed
8. Configuration management practice must be followed to ensure of regular backups and managed version control exists
9. A scheduled vulnerability scan and management practice must be followed
10. Where applicable, 2FA for accessing applications or remote networks must be implemented

8. Internet-Facing Security

This section defines BCIT's technical standard when securing BCIT internet-facing infrastructure. For effective security management, principle of least privilege must be practiced.

Technical Standard #08

BCIT defined internet-facing security practices must adhere to:

1. ACL approach must be followed to block high-risk TCP/UDP ports
2. A default deny-all rule must be configured for each interface in both directions
3. Firewalls protecting assets must perform stateful packet inspection and logging
4. Firewalls must be configured (where applicable) to protect and perform correction actions for content filtering, DLP and malware protection (e.g. block high risk file types, exe, bat, ps1)
5. Firewall features IDS/IPS and WAF must be configured to protect against advanced threats
6. A geofencing practice must be followed to limit noise from and to the internet
7. DNSSEC must be implemented to protect DNS service
8. SPF, DKIM and DMARC must be enabled and configured to protect email
9. Privileged access for management over internet must be disabled
10. 2FA for accessing applications or remote networks must be implemented

9. Logging and Monitoring

This section defines BCIT's technical standard in achieving an effective logging and monitoring practice. This security standard takes into account that continuous monitoring and/or periodic reviews provide ongoing assurance that BCIT systems and the BCIT electronic information, which they hold, are secure and that confidentiality and integrity are effectively being ensured. In the event of a security breach, audit logs are relied upon to determine whether or not information has been accessed or modified without authority.

Technical Standard #09

BCIT defined logging and monitoring for security purposes must adhere to the following:

1. Logs must be enabled and monitored to determine the use of system resources and to detect security events (e.g. failed logons, simultaneous logins from different geographic locations, escalation of privilege, attacks against systems, etc.)
2. All user logins, logouts and access to resources (applications and networks) must be logged
3. All actions (where applicable) performed along with time it was performed must be logged
4. All access (where applicable) to or modification of records must be logged
5. All logs must be protected against unauthorized access and modification
6. All traffic logs to and from Network and Internet-Facing infrastructure must be logged
7. All logs must be retained for 90 days onsite, with an offsite copy available for 180 days

10. Account and Session Management

This section defines BCIT's technical standard in ensuring inactive account access is revoked per a strict and set timeline. Accordingly, inactive sessions must be managed through automated session lock mechanism or set to expire as per the standard.

Technical Standard #10

BCIT defined inactive account and session management for security purposes must adhere to:

1. Upon termination, user accounts must be disabled (i.e. access is revoked) immediately. Accounts must either be disabled or password changed to restrict access to specific users.
2. The information stored in disabled and privileged accounts, as well as the username, logs and other metadata for these accounts, must be retained for 180 days.
3. In order to manage inactive sessions an automated session lock mechanisms respecting 15 minutes of inactivity must be in place to enable locking of the information system session.

11. Privileged Account Management

This section defines BCIT's technical standard when working with privileged accounts. Accordingly, privileged accounts are sensitive and provide a high degree of access and therefore pose a signification risk and must be managed as per the standard.

Technical Standard #11

BCIT defined privileged account management for security purposes must adhere to:

1. Access to privileged accounts must be reviewed and documented annually. Discrepancies must be reported in a timely manner to the CSO.
2. Privileged accounts must not be used for day-to-day activities, such as web browsing on a local PC.
3. Privileged accounts must not be shared between applications or services (except Service Accounts). A separate account must be created for each application/service.

At BCIT, privileged accounts are categorized into the following types:

Privileged Account Type	Description
Privileged Personal Accounts	Accounts assigned to individual users (usually IT Technical Staff). Examples: DBA, Exchange Admins, Domain Admins
Privileged Shared Accounts	Accounts that exist in virtually every device or software application; these accounts hold “super user” privileges and are often shared among IT Technical Staff. Examples: Windows local Administrator, UNIX root, Oracle SYS, sa.
Privileged Service Accounts	Accounts that provide a security context to a running service, daemon or process, such as a file server, web server, e-mail server, etc., or are used by applications to access databases and other applications.
Privileged Emergency Accounts	Accounts used by the enterprise when elevated privileges are required for business continuity and or disaster recovery. Also referred as fire-call accounts.

12. Vulnerability Monitoring and Management

This section defines BCIT's technical standard when reviewing and protecting BCIT systems through vulnerability monitoring and management. A practice designed to proactively reduce the chance of exploitation of system and application related vulnerabilities.

Technical Standard #12

BCIT defined vulnerability monitoring and management for security purposes must adhere to:

1. BCIT ITS teams must subscribe to appropriate notification lists to ensure they are aware of new reported vulnerabilities and corresponding patches as they become available.

2. BCIT must follow Common Vulnerability Scoring System (CVSS v3.0) when rating vulnerabilities as per below classification:
3.

Severity	Base Score Range
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

4. In order to mitigate risk, vulnerabilities must be patched in time as follows:

Severity	Base Score Range	Patch
None	0.0	n/a
Low	0.1 – 3.9	< 7 days
Medium	4.0 – 6.9	< 3 days
High	7.0 – 8.9	< 48 hours
Critical	9.0 – 10.0	< 24 hours

5. Operating system and application updates and patches must be installed as follows:
    a. to the extent possible, desktops, laptops and servers must be configured to install these updates and patches automatically;
    b. where automatic installation is not feasible, all security-related updates and patches must be manually installed at the earliest opportunity, in accordance with their severity, as outlined in #4 above;
    c. where it is impractical or impossible to install security-related updates and patches, the risks must be mitigated with compensating controls approved by the CSO; and
    d. where the system is at end of life and security-related updates and patches are no longer available from the vendor, then you must either upgrade the system or implement compensating controls approved by the CSO.
6. Cyber Security team is responsible for ensuring continuous vulnerability monitoring of all operational systems and applications connected to BCIT networks are scanned for vulnerabilities using authenticated and unauthenticated scans.
7. All new or substantially modified internet-facing systems or applications connected to BCIT network must undergo a vulnerability assessment prior to going into production. Any detected vulnerabilities must be resolved in accordance with the above mentioned #4 severity rating.

Amendment History

1. Created 2019 APR 30
2. Published 2020 June 02

Scheduled Review Date

2021 June 30