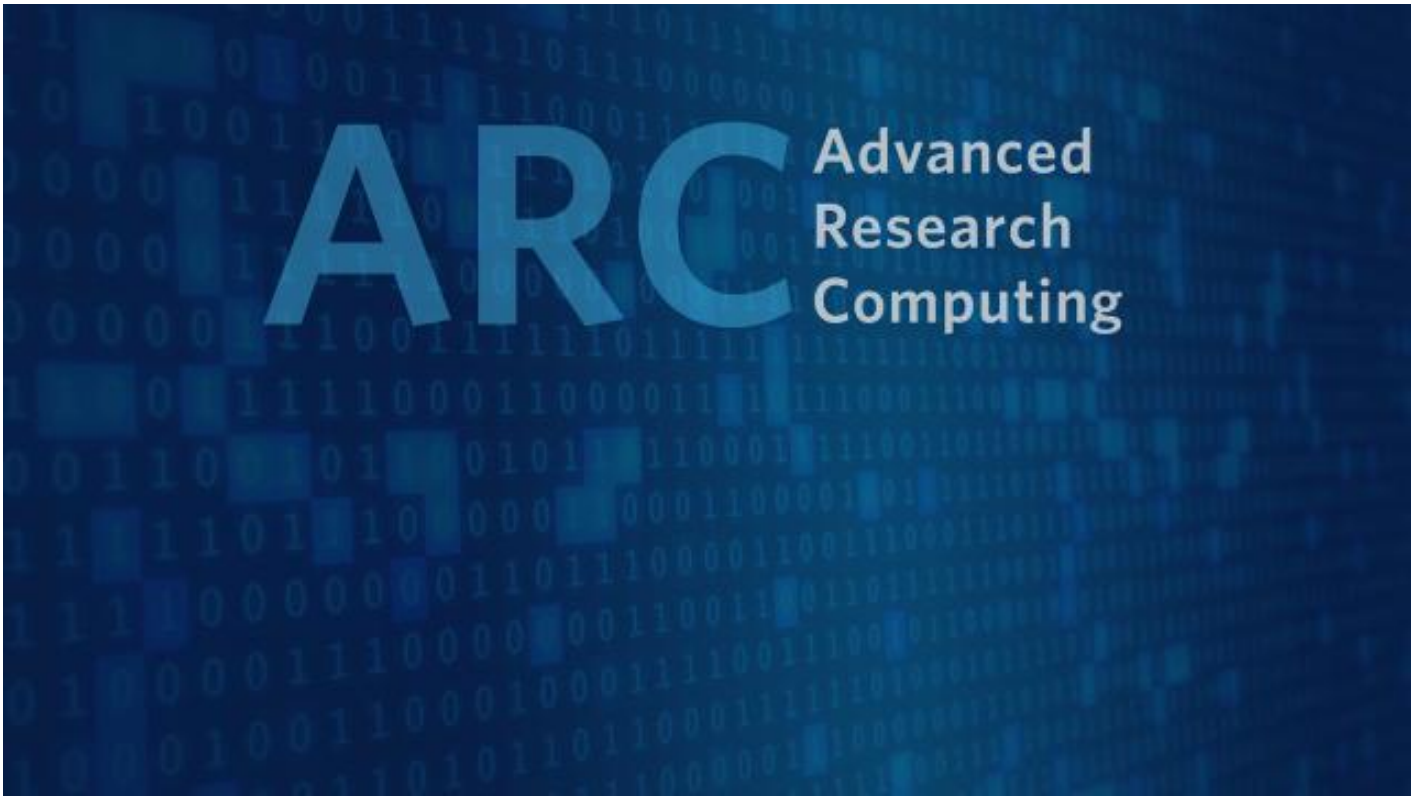
UBC Research Security Compliance Checklist

Version 2.1.0



THE UNIVERSITY OF BRITISH COLUMBIA

ARC Security Compliance Checklist

Preface

The UBC Research Security Compliance Checklist is a self-assessment tool designed to help evaluate the security posture of a solution at a high-level. It contains a list of items to consider for both compliance with UBC Security Policy and Standards, as well as cybersecurity good-practices.

Before you begin

Before you complete this checklist please note:

- This checklist is not solution specific. Some items listed may not apply to your architecture
- It is recommended that the project technical lead and/or solution provider be consulted to complete this document
- This document was created by Advanced Research Computing (ARC) as a self-verification tool. It will **not** be reviewed by a cybersecurity professional.
- This document does **not** constitute a security Threat Risk Assessment (STRA) and should not be used for this purpose. Please visit our website for more information about STRAs: https://arc.ubc.ca/security-privacy

Instructions

1. Identify your Electronic Information classification **and** Electronic Service risk classification using UBC Information Security Standard U1 (ISS-U1).
2. Indicate where the information collected will be stored
3. Identify your solution design
4. Indicate how the solution will be accessed and supported
5. Based on the response provided in Solution Information, complete the required sections of the Security Compliance Checklist.

Need Assistance?

If you need clarifications or guidance to complete this document, please contact arc.support@ubc.ca.

Research Information

Information Classification

Indicate **ALL** information type that will be collected/processed/stored by the solution:

Electronic Information	Examples		Please complete
Contact information of participants	name, physical address, phone number, email address	☐	Section 1 to 6, **AND** See note below **AND** Section 21 (optional)
Personal information of one or multiple individuals **including de-Identified information**	Age, physical location, scraped human (non-health), grades, student records, conversation or focus group transcripts, religious beliefs, political allegiance, socioeconomic data, opinion about a specific topic.	☐	
Photo, video or audio recording of one or multiple individual	Zoom video recordings, focus-group audio recordings, photos or image of students.	☐	
Personal Health-Information **including de-identified information**	Health records, diagnosis, medical imaging, medication, admission date, health service received.	☐	
Physiological information about individuals **including de-identified information**	Date of birth, height, weight, color of eyes, sex assigned at birth, gender identity, ethnicity, genetic data, biometric data, biospecimens.	☐	
Identifying information about an individual	Personal Health Number, MRN, SIN number, student ID, government issued ID number, banking information, criminal record	☐	
Proprietary or confidential information that **IS NOT** personal information	Financial business information/records, trade secrets, system configuration, Novel drug formula in partnership with pharmaceutical company, Software written in conjunction with a commercial partner, Patentable software, sensitive technologies, Animal genomics, Submitted manuscripts that are currently under embargo, Restricted circulation of library journal.	☐	
Payment Card Industry (PCI) information	Debit/credit card numbers, names, expiry dates or PINs	☐	
Published manuscripts, publicly available/aggregated information	Data from the Statistic Canada website, names and business contact info of Faculty or Staff members, Data analysis scripts that is protected by a Non-Disclosure Agreement OR that does not include personal and health information.	☐	Section 1 to 6 **AND** Section 21 (optional)
Non-proprietary, non-human data	Fictitious data, simulation data, computer generated data, measurements over time, particle physics data.	☐	

Note: If the solution collects, store and/or process **any** personal information **including de-identified information**, you may be required to complete a Privacy Impact Assessment (PIA) and/or Security Threat Risk Assessment (STRA). To learn more about PIA and STRA requirements at UBC, visit the UBC Privacy Matters website

Information Storage

Indicate where electronic information associated with the research project or service will be stored:

Electronic Information Storage		Please Complete
This solution does not store any information	☐	
Information is stored using a UBC Storage Service like UBC OneDrive, SharePoint, Teams or TeamShare	☐	
Information is stored **in** the UBC datacenter or datacenter that meets the requirements of UBC ISS-M9	☐	
Information stored using a Commercial Cloud service	☐	Section 9
Information is stored on a Desktop or Laptop	☐	Section 12
Information is stored on a mobile device (e.g.: tablet)		Section 13
Information is stored in UBC Educloud		Section 14
Information is stored on a server, instrument or IoT device residing **outside** the UBC datacenter or Commercial Cloud	☐	Section 14
Information is stored on a mobile/portable storage unit (e.g.: external hard-drive, usb key, NAS)	☐	Section 15

Information Access

Indicate how you will access electronic information associated with the research project or service:

Device type		Please Complete
Desktop(s) or laptop(s) computer(s)	☐	Section 12
Mobile device(s) such as smart phones and tablets	☐	Section 13
Instrument(s) such as a microscope	☐	Section 14
Internet of Things (IoT) device(s)	☐	Section 16

Solution Provider and Support

Indicate who will provide the solution and its support where applicable:

Solution Provider	Description		Please Complete
UBC IT	Check the list of UBC supported platforms to confirm if the solution you are using is provided and supported by UBC IT.	☐	
An IT at UBC group	It at UBC are department and faculty dedicated IT group providing services and/or support to their department/faculty (e.g: FoM Digital Solutions) or to a specific UBC community (e.g.: Advanced Research Computing, CTLT, etc.).	☐	Section 8
An external service provider	External service providers are providers that are not UBC affiliated (e.g.: solution providers (vendors), managed support services, other institutions, developers and and contractors.	☐	
The research group	You should select this option if your research group has developed a custom solution that is being entirely supported by the research group (e.g.: novel technology software using custom codes developed by the research group to achieve x).	☐	

Electronic Service Classification

Please consult UBC ISS-U1 to identify this solution classification:

Electronic Service Classification		Please complete
Low Risk: Loss of confidentiality or availability in a Low Risk Electronic Service would cause minimal impact on to UBC's mission, safety, finances, or reputation.	☐	Section 1 to 6 Section 21 (optional)
Medium Risk: Loss of confidentiality or availability in a Medium Risk Electronic Service would cause minor impact on to UBC mission, safety, finances, or reputation.	☐	Section 1 to 6 Section 21 (optional)
High Risk: Loss of confidentiality or availability in a High Risk Electronic Service would have a significant business impact to the university including one or more portfolios, but not the whole University.	☐	Section 1 to 7 Section 21 (optional)
Very High Risk: Loss of confidentiality or availability in a Very High Risk UBC Electronic Service would have a major business impact to the University.	☐	Section 1 to 7 Section 21 (optional)

Solution design

Indicate which components are present for this solution:

Component		Please Complete
Cloud component(s) including storage and processing	☐	Section 9
Internet-facing component(s)	☐	Section 10
Development instance(s)	☐	Section 11
The solution includes or connect to a database	☐	Section 17
A containerized environment	☐	Section 18
Custom or unique developed codes or components used specifically for the related research project/initiative	☐	Section 19
Artificial Intelligence (AI) or Large Language Model (LLM)	☐	Section 20

Note: Solutions identified as restricted by UBC may require a variance request to be submitted. See UBC Information Security Standard U12 (ISS-U12) for more information.

Security Compliance Checklist

#	Section	Security control or Standard requirement	Reference
1	Password Management	☐ Solution is Password protected; ☐ Passwords are not shared; ☐ Default vendor password(s) were changed following the installation of solution ☐ Password policy and storage is compliant with UBC Security Standard ISS-U2; ☐ Authentication systems does not store account passwords in clear text; ☐ The account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period **OR** Each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the User successfully logs in; ☐ The identity of a user is verified prior to providing a new, replacement or temporary password for an account. ☐ Multi-Factor Authentication (MFA) is enforced (unless not technically feasible)	UBC ISS-M4 & ISS-U2
2	User Account Management	☐ Applications for User Accounts are reviewed and approved; ☐ A record is kept of all users being granted an account and who provided authorization; ☐ All user accounts are uniquely identifiable to specific users; ☐ User accounts are only granted the required access as per the principle of "least privilege"; ☐ User accounts undergo regular risk-based reviews to ensure access is still relevant to users' roles and responsibilities; ☐ User accounts are not shared and are traceable back to the individual using them (except in test and pre-prod environment); ☐ A procedure is in place to disable terminated user accounts (privileged and regular) in a timely manner; ☐ User accounts and authorization records have a retention policy of at least one year after termination.	UBC ISS-M2

3	**Privileged User Account Management**	☐ Privileged accounts are provided access to only the required systems following the principle of "least privilege"; ☐ Service Accounts are not shared between applications or services; ☐ Privileged Accounts are not used for day-to-day activities, such as email and web browsing; ☐ Privileged Accounts are not used (except Service Accounts) to run daemons, services or applications; ☐ Private keys used with Privileged or Service Accounts, are protected in compliance with UBC ISS-M3, ISS-M4, **and** UBC ISS-M7; ☐ Access to Privileged Accounts is reviewed at an interval stipulated by the Technical Owner of the System (in consultation with the Administrative Head of Unit), or at a minimum annually, to validate that they remain restricted to authorized personnel; ☐ IT Support Staff, including vendor staff, with access to Privileged Accounts, have agreed comply with the System Administrators' Code of Ethics.	UBC ISS-M3, ISS-M4 & ISS-M7
4	**Vulnerability Management**	☐ Solution receives feature and security patches (solution is not end-of-life); ☐ Patch management procedures prioritize patches based on the severity of the vulnerability being patched, the sensitivity of the data in the system, and the criticality of the system to University Business; ☐ Patch application policy is compliant with UBC ISS-M5 (critical=within 48h; High=within 14days; Medium & low= asap); ☐ Backups are completed and verified before application of any new patches or updates; ☐ Systems and applications have been enrolled in the UBC Vulnerability Management Service **OR** are regularly scanned to detect new vulnerabilities.	UBC ISS-M5
5	**Logging and Monitoring**	☐ Solution collects security logs; Security logs include: ☐ User login, logout and access to a resource; ☐ Action performed by the User and the time it was performed; ☐ Any access to, or modification of, records; Security logs are: ☐ Stored in UBC MyLogs **OR** Retained for at least 90 days where use of UBC MyLogs is not technically possible; ☐ retrievable in a timely manner if required for analysis; ☐ Securely stored, and protected against unauthorized access and modification.	UBC ISS-M8

6	Data Encryption and cryptographic requirements	☐ Signed x.509 security certificates ☐ Digital signatures are supported by certificates issued by a trusted third-party ☐ Certificate Authority (CA), with a minimum hash algorithm of SHA2; ☐ Cryptographic hash ciphers are using a minimum of: SHA256, SHA512, RipeMD-160, WHIRLPOOL or equivalent, and weak cryptographic hash ciphers are disabled; ☐ Where encryption is used, the encryption layer is AES-256bit or higher; ☐ X.509 certificates are a minimum of 2048-bits. ☐ Cryptographic Keys ☐ Keys are created using cryptographically strong algorithms; ☐ Keys use a strong cryptographic algorithm (minimum AES-256 bit); ☐ Keys are securely stored in a secret vault; ☐ Keys are stored with UBC (and not the vendor) unless not technically possible; ☐ Keys are stored and transmitted using a cryptographic hash and salted (SHA256, SHA512, RipeMD-160, WHIRLPOOL or equivalent); ☐ Keys and their associated software products are securely maintained for the life of the archived data that was encrypted with that product; ☐ Private keys are protected against unauthorized disclosure when using public-private key encryption; ☐ Keys are not stored in the same location as the system the provide access to; ☐ Access and transmission of keys is strictly limited to individuals who have need-to-know; ☐ Where applicable, equipment used to generate, store and archive keys is physically protected; ☐ Documented processes are implemented for key recovery, key changes and revocations; ☐ A documented process is in place to respond to suspected or confirmed compromised keys. ☐ Encryption at-rest ☐ Encryption strength is at a minimum of AES-256bit; ☐ Cryptographic hash ciphers are using SHA256, SHA512, RipeMD-160, WHIRLPOOL or stronger algorithm; ☐ Weak cryptographic hash ciphers are disabled. ☐ Encryption in-transit (in-motion) ☐ All data in transit is encrypted in transit using HTTPS connections (TLS-1.2 or higher).	UBC ISS-U3, ISS-M5, ISS-M7 & ISS-U5

7	High and Very-High criticality services	☐ The service was added to the list of High and Very High Risk services list owned by the administrative head of unit; ☐ The service has undergone a security review prior to deployment; ☐ Where possible, the service architecture include replication to a different region than the primary systems on which the service resides (Not mandatory but recommended); ☐ A documented security incident response plan is in place to ensure the service can be quickly recovered in the event of a security incident (Not mandatory but recommended); ☐ UBC Safety and Risk Services was consulted to ensure a business continuity plan is in place for the service (Not mandatory but recommended).	UBC ISS-U1 & ISS-U7
8	Service Providers and Support	☐ IT at UBC service providers ☐ Support provider user and privileged account(s) meet all criteria listed in section 2 and 3 of this checklist; ☐ Support will be provided for the entire duration of the research project. ☐ External service providers ☐ The Service Provider Security Checklist was completed prior to service providers being provided access to UBC electronic information and systems; ☐ Service provider was informed it will be subject to UBC Systems Policy SC14 and related Standards; ☐ Service provider confirmed they store and transmit UBC Electronic Information in compliance with UBC ISS-U3 and UBC ISS-U5; ☐ Service provider user and privileged account(s) meet all criteria listed in section 2 and 3 of this checklist; ☐ Support will be provided for the entire duration of the research project. ☐ External Service providers with access to High or Very High Risk UBC Electronic Information ☐ The service provider has entered into a service agreement with UBC that includes a Privacy Appendix in the form prescribed by Procurement Services; ☐ Service provider signed a Security and Confidentiality Agreement (SACA) in the form prescribed by the Office of the University Counsel or obtained a waiver from the Office of the University Counsel. ☐ Custom solutions supported by researchers at UBC ☐ ALL user and privileged account(s) meet all criteria listed in section 2 and 3 of this checklist;	UBC ISS-U9, ISS-U3, ISS-U5 & ISS-M3

		☐ The solution and underlying infrastructure access credentials (such as root and service account passwords, private key) are securely stored in a way where they can be retrieved by the solution/service owner; ☐ Maintenance and support for the solution will be provided for the entire duration of the research project or the lifecycle of the solution.	
9	Cloud Storage and Processing	☐ Virtual instances (such as virtual machines, virtual disks, volume images and containers) containing Medium, High or Very High Risk electronic information have Tier 2 encryption enabled; ☐ Virtual instances (such as virtual machines, virtual disks, volume images and containers) are regularly backed up to a secure location and periodically checked for integrity and availability; ☐ All data in transit to and from the cloud is encrypted using secure transfer protocols such as HTTPS connection (TLS-1.2 or higher).	UBC ISS-U5, ISS-U1 & ISS-M7
10	Internet-facing systems	☐ Database servers reside in a different network segment than internet-facing and application servers **OR** use: ▪ A web application firewall; ▪ File integrity monitoring; ▪ Intrusion Detection/intrusion prevention Systems; ▪ Log monitoring (SIEM). ☐ Web servers can only communicate with application servers (not database); ☐ Internet facing servers are placed in a Demilitarized Zone (DMZ) and using firewalls: ▪ Between the DMZ and internet; ▪ Between the DMZ and internal architecture; ▪ Firewall use ingress filtering at minimum; ▪ Firewall uses access rules that restrict traffic to only the minimum necessary to conduct University Business. ☐ DMZ does not contain databases storing High or Very High Risk information; ☐ Internet or Intranet-facing UBC Electronic Services such as websites or Web Applications used to conduct University Business were provisioned within the ubc.ca domain name space, e.g. widget.ubc.ca (where technically possible). ☐ Access to servers hosting Medium, High and Very-High Risk information is limited to users requiring access following the principle of “Least Privilege”; ☐ Internet-facing server(s) underwent a vulnerability scan prior to go live.	UBC ISS-M10

11	**Development**	Development and test environments: ☐ Are isolated from production environment; ☐ Do not use or store production data;	UBC ISS-M11
12	**Endpoint Protection**	Devices used to access the solution: ☐ Have Tier 1 encryption; ☐ Have Tier 2 or tier 3 encryption enforced for UBC Electronic Information stored locally where Tier 1 encryption is not available; ☐ Have Malware and Spyware protection WITH anti-tamper protection enabled (where technically possible); ☐ Operate behind an active Firewall compliant with the UBC Firewalls guideline; ☐ Are password protected following UBC ISS-U2; ☐ Automatically lock after 30 minutes (or less) of inactivity (5min if storing or accessing High or Very-High Risk information); ☐ Run a version of their operating system for which security updates continue to be produced and are available.	UBC ISS-U2, ISS-U5, ISS-M7 & ISS-U7
13	**Mobile Devices (excluding participant devices)**	Mobile devices: ☐ Are password protected following UBC ISS-U2 OR uses a numeric pin of at least 5 characters to unlock; ☐ Mobile devices have Tier 1 encryption; ☐ Have enabled the ability to remotely locate the device in the event of loss or theft (where possible); ☐ Have enabled a feature allowing remote-wipe in the event of loss or theft (where possible); ☐ Have enabled feature for automatic data destruction if more than 10 incorrect passwords are entered (where possible); ☐ Device Bluetooth discovery and pairing have been disabled unless required; ☐ Run a version of their operating system for which security updates continue to be produced and are available.	UBC ISS-U2, ISS-U5, ISS-M7 & ISS-U7

14	**Servers, Instruments and IoT Devices**	Device(s) is(are): ☐ Password protected following UBC ISS-U2; ☐ Device(s) console and/or user interface automatically locks after 5 minutes of inactivity; ☐ Device(s) containing Medium, High or Very High Risk electronic information have Tier 1 encryption enabled; ☐ Virtual instances (such as virtual machines, virtual disks, volume images and containers) containing Medium, High or Very High Risk electronic information have Tier 2 encryption enabled; ☐ Have Malware and Spyware protection; ☐ Have an active Firewall compliant with the UBC Firewalls guideline; ☐ Run a version of their operating system for which security updates continue to be produced and are available; ☐ Are regularly backed up to a secure location and periodically checked for integrity and availability; ☐ Device(s) is(are) physically protected from un-authorized access; ☐ Device(s) is(are) configured to limit traffic ONLY to required connections.	UBC ISS-U2, ISS-U5, ISS-M7 & ISS-U7
15	**Mobile/portable storage**	☐ Have Tier 1 encryption; ☐ Are password protected following UBC ISS-U2; ☐ Are regularly backed up to a secure location and periodically checked for integrity and availability; ☐ Physical security controls are in place to ensure the device(s) is(are) not stolen or otherwise compromised.	UBC ISS-U2, ISS-U5, ISS-M7 & ISS-U7
16	**IoT Devices**	☐ A risk-based approach consistent with UBC ISS-U11 section 2 has been taken when locating the device; ☐ Device was secured against unauthorized physical access (blocked unused USB, Ethernet ports); ☐ Device is password protected following UBC ISS-U2 (including firmware or other management console); ☐ A backup of the device configuration is maintained in a secure location; ☐ Device(s) storing Medium, High or Very-High Risk information is regularly backed up to a secure location and periodically checked for integrity and availability; ☐ All network traffic to or from the device is secured against unauthorized access; ☐ Device(s) are only accessible as permitted in UBC ISS-U11 section 5; ☐ Device is not left in reset, setup or discovery mode;	UBC ISS-U2, ISS-U11 & ISS-U7

		☐ Device Bluetooth discovery and pairing is disabled unless required; ☐ Insecure configurations were remediated prior to the device being used in production; ☐ Unnecessary network services, physical and wireless interfaces have been disabled; ☐ Device storing data has encryption in transit, and at rest, and uses encryption; algorithms that are compliant with UBC ISS-U7; ☐ Run a version of their operating system for which security updates continue to be produced and are available OR has compensating controls approved by the CISO; ☐ Device updates are automated or installed by authorized personnel only; ☐ Any customization of the operating system or firmware of the Device not performed by the manufacturer follows UBC ISS-U11; ☐ Device is monitored for availability and checked for unusual behavior or performance to ensure a timely and appropriate response; ☐ Device is recorded in an inventory, maintained by the User and provided to University IT Support Staff prior to going into production.	
17	**Database and File Encryption**	☐ Tier 3 encryption is enforced for **ALL DATABASES** containing High or Very High Risk electronic information. ☐ Tier 3 encryption is enforced for **ALL File Storages** containing High or Very High Risk electronic information.	UBC ISS-U5
18	**Containerized Environment**	☐ Containers use a container image for which security updates continue to be produced and are available; ☐ Containers are hardened and isolated from their host to mitigate container escape vulnerabilities; ☐ Container access uses secure network communication protocols (such as TLS/SSL); ☐ Access to orchestration systems is limited to authorized personnel only; ☐ The security of the container host system is compliant with the requirements of section 1 to 7, and section 14 of this checklist. **Containerized Environment Encryption:** ☐ Containers storing UBC Electronic Information, including cached information uses encryption that is compliant with UBC ISS-U5 **OR**, ☐ Containers are fully compliant with the criteria below, and they have been documented in a completed and submitted Encryption Exemption Attestation Form: ▪ Containers do not store UBC Electronic Information, including cached information.	UBC ISS-U5, ISS-M8, ISS-M7 & ISS-U7

		▪ Logs containing information needed for security investigation, as outlined in Section 2 of UBC ISS-M8, Logging and Monitoring of UBC Systems are stored outside the container. ▪ Endpoint Detection and Response (EDR) software approved by the CISO has been installed where technically possible.	
19	**Custom Designed Solutions**	☐ The Software Application Security Checklist was completed; ☐ A Privacy Impact Assessment (PIA) and/or Security Threat Risk Assessment (STRA) was completed for the solution; ☐ Where applicable, the OWASP Application Security Verification Standard (ASVS) was reviewed and guidance applied during the development process; ☐ Where applicable, the OWASP Mobile Application Security (MAS) was reviewed and guidance applied during the development process; ☐ Static Code Analysis was performed prior to the solution moving to production; ☐ Code-level security review was conducted with professionally trained peers; ☐ Custom developed solutions validate input properly and restrictively, allowing only those types of input that are known to be correct (e.g. cross-site scripting, buffer overflow errors, SQL injection flaws, etc.); ☐ Custom developed solutions execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system; ☐ Custom developed solutions were scanned before being connected to UBC Network; ☐ Custom developed solutions were provisioned within the ubc.ca domain (where technically possible); ☐ Custom developed solutions have a change management process implemented; ☐ Custom developed solutions securely store and restrict access to application/system documentation; ☐ Where applicable, the SANS CWE TOP 25 Most Dangerous Software Errors were reviewed and considered within the development of the solution.	UBC ISS-M11
20	**Artificial Intelligence (AI) and Large Language Models (LLM)**	☐ The UBC Generative AI Guideline was reviewed and applied; ☐ The solution does **not** utilize DeepSeek (excludes downloading and making use of the DeepSeek model)	UBC ISS-U12

21	Best Practices (optional)	Additional Security Controls: ☐ UBC LDAP integration for user authentication is employed wherever possible; ☐ The system uses Role-based Access Controls (RBAC); ☐ A dedicated/segregated network segment (such as a VPN pool) is in place for privileged access; ☐ Application and database servers reside in separated network segments. Logs monitoring and Auditing: ☐ Security logs are monitored by an administrator on a regular basis; ☐ A (Security Information and Event Management) SIEM or similar is configured to send alerts when unusual activities occur; ☐ Solution undergo periodic internal and external audits. Governance documentation: ☐ Documented onboarding and off-boarding procedures; ☐ Data Management Plan (DMP); ☐ Incident Response Plan. Training and Security Awareness: ☐ Users received training on the solution usage; ☐ Users received basic security and privacy awareness training to recognize potential security threats such as Phishing attacks; ☐ Users received training on how to identify and report cybersecurity incidents.	