

ARC Security Compliance Checklist

Version 1.0.1

ARC Advanced
Research
Computing



THE UNIVERSITY OF BRITISH COLUMBIA

ARC Security Compliance Checklist

Preface

The Security Compliance Checklist is a self-assessment 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 documents was created by Advanced Research Computing (ARC) as a self-assessment tool. It will **not** be reviewed by a Security Analyst.
- This document does **not** constitute a security threat assessment (STA) and should not be used for this purpose. Please contact arc.support@ubc.ca if you would like to obtain an STA.

Instructions

1. Identify your information classification using [UBC Standard #U1](#)
2. Identify your solution design
3. Indicate where the information collected will be stored
4. Indicate if this solution uses mobile or IoT devices
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.

Solution Information

Information Classification

Please consult [UBC Standard #U1](#) to properly identify and classify the data you (will) process or store:

Classification	Please complete
Low Risk: UBC Electronic Information that would cause minimal harm if disclosed, or may be freely disclosed	<input type="checkbox"/> Section 1-6 <input type="checkbox"/> Section 16 (optional)
Medium Risk: UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to UBC or others if released to unauthorized individuals	<input type="checkbox"/> Section 1-7 <input type="checkbox"/> Section 16 (optional)
High Risk: UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction, and could cause moderate harm if disclosed	<input type="checkbox"/> Section 1-7 <input type="checkbox"/> Section 16 (optional)
VeryHigh Risk: UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction, and could cause significant harm if disclosed	<input type="checkbox"/> Section 1-7 <input type="checkbox"/> Section 16 (optional)

Solution design

Solution was designed by an external provider (Vendor)	<input type="checkbox"/> Section 8
Solution was custom designed internally by the project team	<input type="checkbox"/> Section 9
Solution has web-facing application(s) and/or server(s)	<input type="checkbox"/> Section 10

Information Storage

This solution does not store any information	<input type="checkbox"/>
Information is stored in the UBC datacenter or datacenter that meets the requirements of Security Standard #M9	<input type="checkbox"/>
Information is stored on a server or computer residing outside the UBC datacenter or datacenter that meets the requirements of Security Standard #M9	<input type="checkbox"/> Section 11
Information is using Cloud storage and/or processing (SaaS, PaaS, IaaS)	<input type="checkbox"/> Section 12
Information is stored on a mobile/portable storage unit (including NAS)	<input type="checkbox"/> Section 13

Mobile and IoT devices

Solution uses mobile device(s)	<input type="checkbox"/> Section 14
Solution uses IoT device(s)	<input type="checkbox"/> Section 15

Security Compliance Checklist

#	Category	Security control or Standard requirement	Reference
1	Password Management	<input type="checkbox"/> Solution is Password protected <input type="checkbox"/> Passwords are not shared <input type="checkbox"/> Default vendor password(s) were changed following the installation of solution <input type="checkbox"/> Password policy and storage is compliant with UBC Security Standard #U2 <input type="checkbox"/> Authentication systems does not store account passwords in clear text <input type="checkbox"/> 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. <input type="checkbox"/> The identity of a user is verified prior to providing a new, replacement or temporary password for an account	UBC Security Standard #M4 & #U2
2	User Account Management	<input type="checkbox"/> Applications for User Accounts are reviewed and approved <input type="checkbox"/> A record is kept of all users being granted an account and who provided authorization <input type="checkbox"/> All user accounts are uniquely identifiable to specific users <input type="checkbox"/> User accounts are only granted the required access as per the principle of “least privilege” <input type="checkbox"/> User accounts undergo regular risk based reviews to ensure access is still relevant to user role and responsibility <input type="checkbox"/> User accounts are not shared and traceable back to the individual using them (except in test and pre-prod environment) <input type="checkbox"/> A procedure is in place to disable terminated user accounts (privileged and regular) in a timely matter. <input type="checkbox"/> The user account and authorization record has a retention policy of at least one year <input type="checkbox"/> Disabled user accounts have data retention policy of at least one year	UBC Security Standard #M2
3	Privileged User Account Management	<input type="checkbox"/> Privileged accounts are provided access to only the required systems as per the principle of “least privilege” <input type="checkbox"/> Service Accounts are not shared between applications or services <input type="checkbox"/> Privileged Accounts are not used for day-to-day activities, such as email and web browsing <input type="checkbox"/> Privileged Accounts are not used (except Service Accounts) to run daemons, services or applications	UBC Security Standard #M4 & #M7

		<input type="checkbox"/> Private keys used with Privileged Accounts, are protected in compliance with UBC Security Standard #M4 - Securing User Account and UBC Security Standard #M7 - Cryptographic Controls . <input type="checkbox"/> 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 <input type="checkbox"/> IT Support Staff, including vendor staff, with access to Privileged Accounts, have agreed comply with the System Administrators' Code of Ethics .	
4	Endpoint Protection	Devices used to access the solution: <input type="checkbox"/> Have full disk encryption (Laptop and Desktop computers) <input type="checkbox"/> Have Malware and Spyware protection <input type="checkbox"/> Operate behind an active Firewall compliant with the UBC Firewalls guideline <input type="checkbox"/> Are password protected following UBC Security Standard #U2 <input type="checkbox"/> Automatically lock after 30 minutes (or less) of inactivity (5min if storing or accessing High or Very-High Risk information) <input type="checkbox"/> Run a version of their operating system for which security updates continue to be produced and are available	UBC Security Standard #U2 , #U5 & #U7
5	Vulnerability Management	<input type="checkbox"/> Solution receives security patches <input type="checkbox"/> 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. <input type="checkbox"/> Patch application policy is compliant with UBC Security Standard #M5 - Vulnerability Management (critical=within 48h; High=within 14days; Medium & low= asap) <input type="checkbox"/> Backups are completed and verified before application of any new patches or updates	UBC Security Standard #M5
6	Logging and Monitoring	<input type="checkbox"/> Solution collects security logs Security logs include: <input type="checkbox"/> User login, logout and access to a resource <input type="checkbox"/> Action performed by the User and the time it was performed <input type="checkbox"/> Any access to, or modification of, records Security logs are: <input type="checkbox"/> Retained for at least 90 days <input type="checkbox"/> retrievable in a timely manner if required for analysis <input type="checkbox"/> Protected against unauthorized access and modification	UBC Security Standard #M8

7	Data Encryption and cryptographic requirements	<input type="checkbox"/> Data is encrypted in transit using HTTPS connection (TLS-1.2 or higher) <input type="checkbox"/> Data stored outside the UBC Data Centre OR datacenter that meet requirements of UBC Security Standard #M9 is encrypted at rest using AES-128 bit or higher <input type="checkbox"/> Solutions using digital certificates employ a minimum hash algorithm of SHA2 <input type="checkbox"/> Solution is protected by a firewall and compliant with required configuration from UBC Security Standard #M5	UBC Security Standard #U3 , #M5 , #M7 & #M9
8	Service Provider support and system access	<input type="checkbox"/> Service provider completed the Service Provider Security Risk Assessment prior of being provided access to UBC electronic information and systems <input type="checkbox"/> Service provider signed a Security and Confidentiality Agreement (If provided access to Medium, High or Very-High Risk information) <input type="checkbox"/> Service provider was advised they will be subject to UBC Policy SC14 and related Standards <input type="checkbox"/> Service provider does not access or store personal information outside Canada <input type="checkbox"/> Service provider user and privileged account(s) meet all criteria listed in section 2 and 3 of this checklist	UBC Security Standard #U9
9	Development	Development and test environments: <ul style="list-style-type: none"> <input type="checkbox"/> Are isolated from production environment <input type="checkbox"/> Do not use or store production data Custom developed applications: <ul style="list-style-type: none"> <input type="checkbox"/> 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.) <input type="checkbox"/> Execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system <input type="checkbox"/> Were scanned before being connected to UBC Network <input type="checkbox"/> Were provisioned within the ubc.ca domain (unless not technically possible) <input type="checkbox"/> Have a change management process implemented <input type="checkbox"/> Securely store and restrict access to application/system documentation 	UBC Security Standard #M11
10	Internet-facing systems	<input type="checkbox"/> Web application and database are hosted on separate servers OR use: <ul style="list-style-type: none"> - A web application firewall - File integrity monitoring - Intrusion Detection/intrusion prevention Systems - Log monitoring (SIEM) <input type="checkbox"/> Web servers can only communicate with application servers (not database) <input type="checkbox"/> Internet facing servers are placed in a Demilitarized Zone (DMZ) and using firewalls:	UBC Security Standard #M10

		<ul style="list-style-type: none"> - 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 <p><input type="checkbox"/> DMZ does not contain databases storing High or Very High Risk information.</p> <p><input type="checkbox"/> Access to servers hosting Medium, High and Very-High Risk information is limited to users requiring access as per the principle of “Least Privilege”</p> <p><input type="checkbox"/> Internet-facing server(s) underwent a vulnerability scan prior to go live</p>	
11	Server storage	<p>Server or desktop storing UBC Electronic Information, and residing outside the UBC Datacenter or datacenter with similar configuration have the following controls:</p> <p><input type="checkbox"/> Password protected following UBC Security Standard #U2</p> <p><input type="checkbox"/> Server console and/or user interface automatically locks after 5minutes of inactivity</p> <p><input type="checkbox"/> Have full disk encryption (if storing Medium, High or Very High Risk information)</p> <p><input type="checkbox"/> Have Malware and Spyware protection</p> <p><input type="checkbox"/> Have an active Firewall compliant with the UBC Firewalls guideline</p> <p><input type="checkbox"/> Run a version of their operating system for which security updates continue to be produced and are available</p> <p><input type="checkbox"/> Are regularly backed up to a secure location and periodically checked for integrity and availability.</p>	<p>UBC Security Standard #U2, #U5 & #U7</p>
12	Cloud Storage and Processing	<p><input type="checkbox"/> Virtual servers in IaaS infrastructure have full volume encryption</p> <p><input type="checkbox"/> Virtual Servers are regularly backed up to a secure location and periodically checked for integrity and availability.</p> <p><input type="checkbox"/> SaaS and PaaS environment storing and/or processing High or very-High risk information use at rest encryption of AES-128 bit or higher</p>	<p>UBC Security Standard #U5</p>
13	Mobile/portable storage	<p><input type="checkbox"/> Have device level encryption</p> <p><input type="checkbox"/> Are password protected following UBC Security Standard #U2</p> <p><input type="checkbox"/> Are regularly backed up to a secure location and periodically checked for integrity and availability.</p>	<p>UBC Security Standard #U2, #U5 & #U7</p>
14	Mobile Devices	<p>Mobile device:</p> <p><input type="checkbox"/> password protected following UBC Security Standard #U2 OR uses a numeric pin of at least 5 characters to unlock</p> <p><input type="checkbox"/> Have device level encryption</p>	<p>UBC Security Standard #U2, #U5 & #U7</p>

		<ul style="list-style-type: none"> <input type="checkbox"/> Have enabled the ability to remotely locate the device in the event of loss or theft (where possible) <input type="checkbox"/> Have enabled a feature allowing remote-wipe in the event of loss or theft (where possible) <input type="checkbox"/> Have enabled feature for automatic data destruction if more than 10 incorrect passwords are entered (where possible) <input type="checkbox"/> Device Bluetooth discovery and pairing is disabled unless required <input type="checkbox"/> Run a version of their operating system for which security updates continue to be produced and are available 	
15	IoT Devices	<ul style="list-style-type: none"> <input type="checkbox"/> A risk based approach consistent with UBC Security Standard #U11 section 2 has been taken when locating the device. <input type="checkbox"/> Device was secured against unauthorized physical access (blocked unused USB, Ethernet ports) <input type="checkbox"/> Device is password protected following UBC Security Standard #U2 (including firmware or other management console) <input type="checkbox"/> A backup of the device configuration is maintained in a secure location <input type="checkbox"/> 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. <input type="checkbox"/> All network traffic to or from the device is secured against unauthorized access <input type="checkbox"/> Device(s) are only accessible as permitted in UBC Standard #U11 section 5. <input type="checkbox"/> Device is not left in reset, setup or discovery mode <input type="checkbox"/> Device Bluetooth discovery and pairing is disabled unless required <input type="checkbox"/> Insecure configurations were remediated prior to the device being used in production <input type="checkbox"/> Unnecessary network services, physical and wireless interfaces have been disabled <input type="checkbox"/> Device storing data has encryption in transit, and at rest, and uses encryption algorithms that are compliant with UBC Security Standard #M7 <input type="checkbox"/> 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 <input type="checkbox"/> Device updates are automated or installed by authorized personnel only <input type="checkbox"/> Any customization of the operating system or firmware of the Device not performed by the manufacturer is in compliance with UBC Security Standard #M11. <input type="checkbox"/> Device is monitored for availability and checked for unusual behavior or performance to ensure a timely and appropriate response <input type="checkbox"/> Device is recorded in an inventory, maintained by the User and provided to University IT Support Staff prior to going into production. 	<p>UBC Security Standard #U2, #U11, #M7 & #M11</p>

16	Best Practices (optional)	<p>Additional Security Controls:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Multi-Factor Authentication is used whenever possible <input type="checkbox"/> UBC LDAP integration for user authentication is employed wherever possible <input type="checkbox"/> The system uses Role-based Access Controls (RBAC) <input type="checkbox"/> Privileged access is segregated <input type="checkbox"/> Application and database servers are separated <input type="checkbox"/> Encryption algorithms used is AES-256 or higher <p>Logs monitoring and Auditing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Security logs are monitored by an administrator on a regular basis <input type="checkbox"/> A (Security Information and Event Management) SIEM or similar is configured to send alerts when unusual activities occur. <input type="checkbox"/> Solution undergo periodic internal and external audits <p>Governance documentation:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Documented onboarding and off-boarding procedures <input type="checkbox"/> Data Management Plan (DMP) <input type="checkbox"/> Incident Response Plan <p>Training and Security Awareness:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Users received training on the solution usage <input type="checkbox"/> Users received basic security and privacy awareness training to recognize potential security threats such as Phishing attacks. <input type="checkbox"/> Users received training on how to identify and report cybersecurity incidents 	
----	---------------------------	---	--