Cyber Security Standard – Risk Management

Version	Approved by	Approval date	Effective date	Next full review
X.X	Vice Chancellor	XX Month Year	XX Month Year	Month Year

Standard Statement

Purpose	The purpose of this Standard is to: a) establish UNSW cyber security risk ratings for Information Resources, and ensure that cyber security risks are appropriately identified, assessed, reported, and treated, consistent with the UNSW Risk Management Framework as well as applicable laws, regulations, standards, and contractual obligations. b) define the minimum set of controls that are required for UNSW Information Resources, consistent with the type of resource and its risk rating. c) provide the linkage between the *Cyber Security Policy* and other Cyber Security Standards that provide additional details.
Scope	This Standard applies to all: a) users of UNSW Information Resources, including but not limited to staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments, affiliates, collaborative researchers, and visitors to the University. b) university-owned, controlled, or leased locations where UNSW Information Resources are located or used. c) UNSW digital information and UNSW Information Resources. d) devices connected to a UNSW network or used to access UNSW Information Resources.
Are Local Documents on this subject permitted?	☐ Yes, however Local Documents must be consistent with this University-wide Document	☒ No

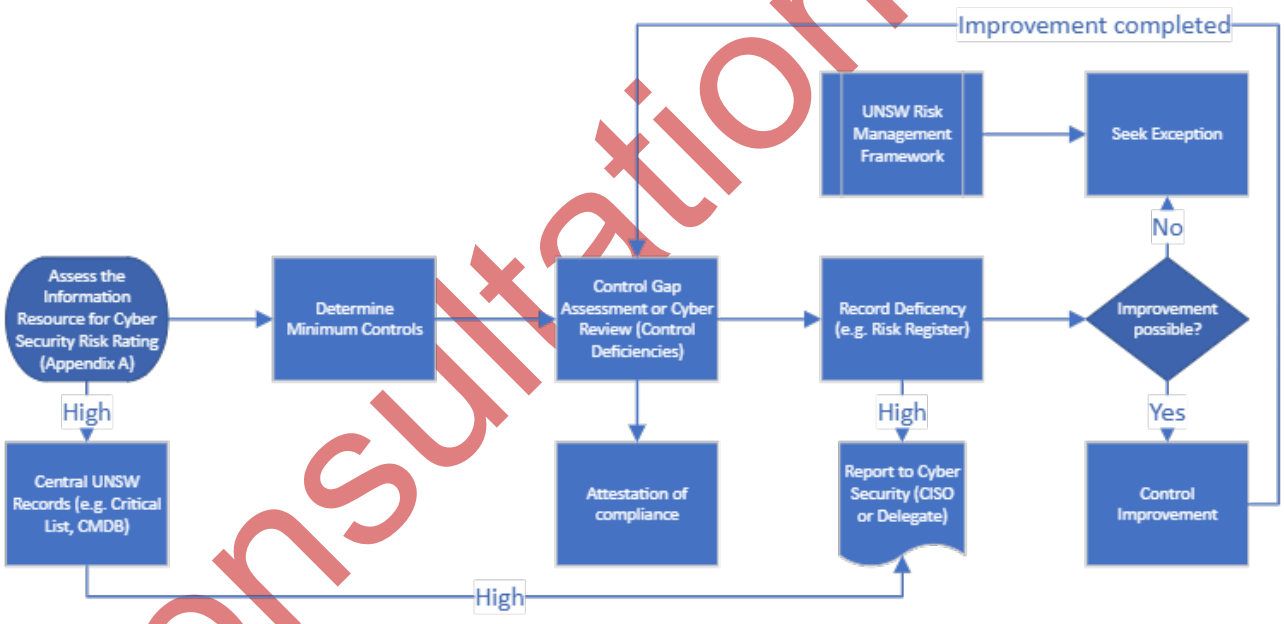
Standard

Table of Contents

1. Risk Management Process

1.1. Cyber security risk within UNSW must be managed in accordance with the process below, and relevant sections within this Standard.

Figure 1 – Cyber Security Risk Management Process



2. Assess and Record Cyber Security Risk Rating

2.1. Business Owners and any other person accountable for designing, building, acquiring, operating, or maintaining a UNSW Information Resource must:

a) determine its cyber security risk rating in accordance with Section 9 (Appendix A) or through consultation with the Chief Information Security Officer, or delegate.

b) maintain records of their Information Resources, cyber security risk rating, and the basis of determination.

c) report Information Resources that a have a high cyber security risk rating to UNSWIT by:

- recording the Information Resource in a Cyber Critical Systems list maintained by the Chief Information Security Officer, or delegate; or a centralised asset inventory (CMDB) maintained by UNSWIT.

- reporting the Information Resource to the Chief Information Security Officer, or delegate to comply with critical infrastructure laws and regulations.

2.2. Deans, Head of Schools, Heads of Research Centres, and Heads of Administrative Units must ensure their unit complies with section 2.1(b).

3. Determine Minimum Controls

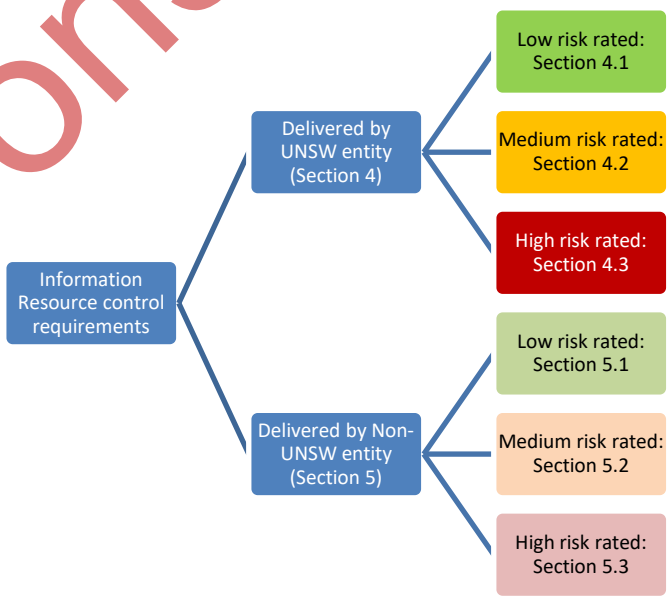
3.1. In this Standard three levels of cyber security risk are defined in Section 9 (Appendix A) and are determined in Section 3.

a) Low cyber security risk-rated Information Resources, where there are limited controls.

b) Medium cyber security risk-rated Information Resources, where a baseline of minimal defensible controls is applied.

c) High cyber security risk rated Information Resources, that have elevated controls needed to support legal, regulatory, and contractual obligations, and industry good practice.

3.2. Business Owners must ensure that cyber security controls are selected and implemented for all UNSW Information Resources within their area of accountability, based upon the cyber security risk rating, and the respective minimum controls in Sections 4 and 5.



a) Information Resources delivered by a UNSW entity must have minimum controls within Section 4.1 – 4.3.

b) Information Resources delivered by a non-UNSW entity under a contractual arrangement must have minimum controls within Section 5.1 – 5.3.

c) Information Resources delivered by both a UNSW entity and non-UNSW entity (hybrid) must have minimum controls from Section 4 and Section 5 based on who delivers each Information Asset or group of assets.

3.3. For Information Resources delivered by a non-UNSW entity, Business Owners must also comply with the *Cyber Security Standard – Vendor Risk Management* including the requirement for new medium and High risk-rated Information Services to have an initial risk and security assessment performed by UNSWIT Cyber Security Governance.

3.4. Additional controls may be required for Information Resources that need to comply with a specific industry standard or contractual obligation such as the Defence Industry Security Program (DISP) or Payment Card Industry – Data Security Standard (PCI-DSS). Guidance should be obtained from the UNSWIT Cyber Security Governance Manager for necessary additional controls.

4. Minimum Controls for Information Resources delivered by a UNSW entity

4.1. Information Resources with a low cyber security risk rating delivered by a UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard - Data Security*.	✓	✓	✓	✓	✓	✓	✓	Data Security
Incident Management	Report cyber security incidents to the UNSWIT Service Desk.	✓	✓	✓	✓	✓	✓	✓	Incident Management
Anti-Malware	Install Anti-Virus protection on all Information Assets, and configure it to scan in real-time, and update daily.			✓	✓	✓	✓	✓	Threat and Vulnerability Management
Approved Email Service	Use UNSWIT Office 365 for Email for any Information Service or Information Asset that sends or receives emails.	✓	✓	✓	✓	✓	✓	✓	Secure by Design

4.2. Information Resources with a medium cyber security risk rating delivered by a UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Single Sign On	Use UNSW Single-Sign On.	✓	✓	✓	✓	✓	✓	✓	Access Control
Passwords	Authentication services must enforce UNSW password policies.	✓	✓	✓	✓	✓	✓	✓	Access Control
Privileged Access Management	Ensure access to privileged administrative (sys admin) and elevated business functions is restricted to those with a documented and approved business or technical need. Use separate credentials for privileged administrative functions and normal user functions. Tools with Privileged Access (System Admin) must be approved by the Business Systems Owner and be controlled and monitored.	✓	✓		✓	✓	✓	✓	Access Control
Remote Access	Use centralised Remote Access Services provided by UNSWIT or Cloud Service Provider (for IaaS, PaaS, or SaaS hosted), including encrypted VPN and multi-factor authentication (MFA). Restrict remote services to the least functionality required.	✓	✓	✓	✓	✓	✓	✓	Access Control
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard - Data Security*.	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption in Transit	Encrypt all authentication data in transit.	✓	✓	✓	✓	✓	✓	✓	Data Security
Incident Management	Report cyber security incidents to the UNSW IT Service Desk.	✓	✓	✓	✓	✓	✓	✓	Incident Management
Asset Inventory	For Information Services – Identify and record all Information Assets and update as assets in the service change.	✓	✓	✓	✓	✓	✓	✓	Information Asset Management
Network Intrusion Detection	For network Services – monitor network traffic for anomalous and potentially suspicious data transfers. UNSWIT-managed networks must include IDS/IPS agents with monitoring by a central SOC.		✓					✓	Network Security
Network Security (Baseline)	Only use UNSWIT Network Services or UNSWIT-approved networks. Install a firewall at the network boundary (connect to external networks only through managed interfaces). Configure network devices in accordance with the *Cyber Security Standard – Network Security*.		✓					✓	Network Security

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Change Control	Use a documented change control process that includes change documentation, change records, a security review, technical and business approval, and controlled release through separate development/test and production environments. *** Changes to one individual endpoint device do not need a formal change control process.	✓	✓	***	✓	✓	✓	✓	Secure by Design
SDLC	For any code developed as part of an Information Service, follow a documented system development lifecycle (SDLC) process that includes requirements, design, development, testing, and implementation stages that include cyber security testing/reviews. Conduct code reviews for application changes and any high-risk security issues must be remediated prior to deployment to production. Highly sensitive data in non-production environments must be sanitised (data masked, tokenised, or scrambled).	✓	✓		✓	✓	✓	✓	Secure by Design
Approved Email Service	Use Office 365 for Email (with Email Online Protection) for any Information Service or Information Asset that sends or receives emails.	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Anti-Malware	Install Anti-Virus protection on all Assets, and configure it to scan in real-time, and update daily.			✓	✓	✓	✓	✓	Threat and Vulnerability Management
Endpoint Detect and Respond Agents (EDR)	Install UNSW Endpoint Detection & Response (EDR) agents on all workstations and servers.			✓	✓		✓		Threat and Vulnerability Management
Software Asset Management Agents (SAM)	Install UNSW Software Asset Management (SAM) agents on all workstations and servers.			✓	✓				Threat and Vulnerability Management
Vulnerability and Patch Management	Identify any vulnerabilities from a reputable source or using vulnerability scanning. Assess the risk of vulnerabilities and install any required software and firmware updates in a timely manner.	✓	✓	✓	✓	✓	✓	✓	Threat and Vulnerability Management

4.3. Information Resources with a high cyber security risk rating delivered by a UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Single Sign On	Use UNSW Single-Sign On.	✓	✓		✓	✓	✓	✓	Access Control
Passwords	Authentication services must enforce UNSW password policies.	✓	✓	✓	✓	✓	✓	✓	Access Control
Multi-Factor Authentication	Use compliant multi-factor authentication (MFA) for all access.	✓	✓	✓	✓	✓	✓	✓	Access Control
Privileged Access Management / Least Privilege	Ensure access to privileged administrative (sys admin) and elevated business functions is restricted to those with a documented and approved business or technical need. Use separate credentials for privileged administrative functions and normal user functions. Tools with Privileged Access (Sys Admin) must be approved by the Business Systems Owner and be controlled and monitored.	✓	✓	✓	✓	✓	✓	✓	Access Control
Remote Access	Use centralised Remote Access Services provided by UNSWIT or Cloud Service Provider providing IaaS, PaaS or SaaS hosting, including encrypted VPN and multi-factor authentication (MFA). Restrict remote services to the least functionality required.	✓	✓	✓	✓	✓	✓	✓	Access Control
Role-Based Training	For Information Services - Ensure users with privileged access (system administration) (including third parties) or elevated business access have security training prior to granting access.	✓	✓	✓	✓	✓	✓	✓	Access Control
Segregation of Duties	Segregate access to minimise the occurrence of errors or unauthorised privileged operations.	✓	✓	✓	✓	✓	✓	✓	Access Control
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard – Data Security*.	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption at Rest	Encryption must be applied in accordance with the *Cyber Security Standard – Data Security*.		✓	✓	✓	✓	✓	✓	Data Security
Encryption in Transit	Encrypt all data in transit outside the network segment or VLAN where Information Asset is located.	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption Key Management	Manage cryptographic keys in accordance with the *Cyber Security Standard – Data Security*	✓	✓	✓	✓	✓	✓	✓	Data Security

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Incident Management	Report cyber security incidents to the UNSW IT Service Desk.	✔	✔	✔	✔	✔	✔	✔	Incident Management
Asset Inventory	For Information Services – Record/register Information Service in a centralised UNSW-wide inventory (CMDB) including ownership, data classification, business impact assessment, risk rating, and location. Update as underlying assets in the service change. Registration may involve legal and regulatory compliance requirements.	✔	✔	✔	✔	✔	✔	✔	Information Asset Management
Business Continuity Plan	Document and annually test a Business Continuity Plan for the service, that addresses loss of location, personnel, technology and any third party required for operation and support of the service.	✔	✔	✔	✔	✔	✔	✔	Information Asset Management
End of Life / End of Support	Do not use end-of-life or end-of-support hardware or software with the Service. Once identified any end-of-life or end-of-support hardware or software must be segmented from the rest of the network.	✔	✔	✔	✔	✔	✔	✔	Information Asset Management
Security Documentation	Develop a service management plan/service handbook that describes system boundaries, system environments, connections with other systems, and what / how security controls are implemented and how they are operated.	✔	✔			✔	✔	✔	Information Asset Management
Physical and Environmental Controls	Use an approved Data Centre, Cloud Service, or ensure compliant physical and environmental controls are in place.		✔	✔	✔	✔	✔	✔	IT Hosting
Security Event Logging	For critical assets, log all required security events to the UNSW Centralised SIEM solution. For all other High risk rated Information Resources, log all required security events to a centralised log management solution. Synchronise internal system clocks with an authoritative (UNSW, IaaS Vendor, or Government) time source.	✔	✔	✔	✔	✔	✔	✔	Logging and Monitoring
Security Event Monitoring	For critical assets, utilise the UNSW Security Operations Centre (SOC). For all other High risk rated Information Resources, utilise a compliant Managed Service Provider (or the service provider of any managed hosting), to monitor logs.	✔	✔	✔	✔	✔	✔	✔	Logging and Monitoring

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Denial of Service	Ensure Denial of Service (DoS) protection is included in hosting, logging capacity is sufficient to meet Standards, and service resilience meets RTO / RPO.		✓					✓	Network Security
Network Intrusion Detection	Monitor network traffic for anomalous and potentially suspicious data transfers. UNSWIT-managed networks must include IDS/IPS agents with monitoring by a central SOC.		✓					✓	Network Security
Network Security	Only use UNSWIT Network Services or UNSWIT-approved networks. Install a firewall at the network boundary (connect to external networks only through managed interfaces). Configure network devices in accordance with the *Cyber Security Standard - Network Security*.		✓					✓	Network Security
Network Segmentation	Implement subnetworks for workloads with different risks/functions. Only allow access from explicitly defines domains, or IP addresses.		✓		✓	✓	✓	✓	Network Security
Networks - Wireless	Wireless access must be authenticated, encrypted, and connected to SIEM and intrusion detection systems are implemented to identify rogue wireless devices and compromises.		✓						Network Security
Web Application Firewall	Use a Web Application Firewall (WAF) in front of all externally facing Information Services, if required by the Chief Information Security Officer as part of a risk treatment, in accordance with the *Cyber Security Standard – Risk Management*.	✓	✓			✓	✓	✓	Network Security
Baseline Configuration	Use a UNSW Baseline Configuration (SOE) or a compliant baseline configuration provided by a Cloud Service Provider (CSP) or research partner.	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Change Control	Use a documented change control process that includes change documentation, change records, a security review (by UNSWIT for high risk), technical and business approval, and controlled release through separate development/test and production environments. *** One individual Information Asset does not need change control.	✓	✓	***	✓	✓	✓	✓	Secure by Design
Enterprise Security Architecture	For Information Services - Use security architecture, designs, and specifications that are consistent with the Enterprise Security Architecture (ESA) and accurately and completely describe compliant security functionality.	✓	✓	✓	✓	✓	✓	✓	Secure by Design

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
SDLC	For any code developed as part of an **Information Service**, follow a documented system development lifecycle (SDLC) process that includes requirements, design, development, testing, and implementation stages that include cyber security testing/reviews. Conduct code reviews for application changes and any high-risk security issues must be remediated prior to deployment to production. Highly sensitive data in non-production environments must be sanitised (data masked, tokenised, or scrambled).	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Approved Email Service	Use Office 365 for Email (with Email Online Protection) for any Information Service or Information Asset that sends or receives emails.	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Backup and Recovery	Create and securely store backups based on business system owner agreed backup cycles (daily, weekly, monthly). Encrypt backups where required. Establish immutable backup (fixed, unchangeable and can never be deleted) where required. Conduct periodic restoration testing.	✓	✓	✓	✓	✓	✓	✓	Secure Continuity
Disaster Recovery Plan	Establish compliant Disaster Recovery infrastructure (for all services other than with recovery time objective (RTO) and recovery point objective (RPO) consistent with those required for business continuity. Document and test-related Disaster Recovery Plans on at least an annual basis.	✓	✓		✓	✓	✓	✓	Secure Continuity
Anti-Malware	Install Anti-Virus protection on all Assets, and configure it to scan in real-time, and update daily.			✓	✓	✓	✓	✓	Threat and Vulnerability Management
Endpoint Detect and Respond Agents (EDR)	Install UNSW Endpoint Detection & Response (EDR) agents on all workstations and servers.			✓	✓		✓		Threat and Vulnerability Management
Penetration Testing	Conduct independent penetration testing annually and with any subsequent significant change, for any externally facing service. Remediate findings in a timely manner.	✓	✓		✓	✓	✓	✓	Threat and Vulnerability Management

Control	What to Do	Applications	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, Containers, and Serverless)	Data and Storage Services	Cyber Security Services,	Hosting Platforms, including ESX Hosts, Data Centres	Where to go for further information
Software Asset Management Agents (SAM)	Install UNSW Software Asset Management (SAM) agents on all workstations and servers.			✔	✔				Threat and Vulnerability Management
Vulnerability and Patch Management	All vulnerabilities must be identified (from vulnerability scanning or reputable sources) and assessed for risk to the service. Install any required software and firmware updates related to the vulnerabilities in a timely manner and in accordance with the Threat and Vulnerability Standard.	✔	✔	✔	✔	✔	✔	✔	Threat and Vulnerability Management
Vulnerability Scanning	For Information Services - Conduct regular (monthly) vulnerability scanning university-approved tools on high-risk Information Resources with findings recorded in a risk register and actions initiated in a ticketing system.	✔	✔	✔	✔	✔	✔	✔	Threat and Vulnerability Management

5. Minimum Controls for Information Resources delivered by a non-UNSW entity

5.1. Information Resources with a low cyber security risk rating delivered by a non-UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard - Data Security.*	✓	✓	✓	✓	✓	✓	✓	Data Security
Incident Management	Report cyber security incidents to the UNSWIT Service Desk.	✓	✓	✓	✓	✓	✓	✓	Incident Management
Anti-Malware	Install Anti-Virus protection on all Information assets, and configure it to scan in real-time, and update daily.	✓		✓	✓	✓	✓	✓	Threat and Vulnerability Management
Approved Email Service	Send and receive Email through a secure email service with content filtering in place.	✓	✓	✓	✓	✓	✓	✓	Secure by Design

5.2. Information Resources with a medium cyber security risk rating delivered by a non-UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Single Sign On	Use UNSW Single-Sign On.	✓	✓	✓	✓	✓	✓	✓	Access Control
Passwords	Authentication services must enforce UNSW password policies or higher	✓	✓	✓	✓	✓	✓	✓	Access Control
Privileged Access Management / Least Privilege	Ensure access to privileged administrative (sys admin) and elevated business functions is restricted to those with a documented and approved business or technical need. Use separate credentials for privileged administrative functions and normal user functions. Tools with Privileged Access (System Admin) must be approved, controlled, and monitored.	✓	✓	✓	✓	✓	✓	✓	Access Control
Remote Access	Use centralised Remote Access Services provided by Cloud Service Provider (for IaaS, PaaS, or SaaS), including encrypted VPN and multi-factor authentication (MFA). Restrict remote services to the least functionality required.	✓	✓	✓	✓	✓	✓	✓	Access Control
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard. - Data Security.*	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption in Transit	Encrypt all authentication data in transit.	✓	✓	✓	✓	✓	✓	✓	Data Security
Incident Management	Report cyber security incidents to the UNSW IT Service Desk.	✓	✓	✓	✓	✓	✓	✓	Incident Management
Asset Inventory	For Information Services – Identify and record all Information Assets and update as assets in the service change.	✓	✓	✓	✓	✓	✓	✓	Information Asset Management
Software Asset Management Agents (SAM)	For workstations and servers delivered to UNSW - install UNSWIT Software Asset Management (SAM) agents			✓	✓				Information Asset Management
Network Intrusion Detection	Network Services – monitor network traffic for anomalous and potentially suspicious data transfers.	✓	✓					✓	Network Security

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Network Security (Baseline)	Install a firewall at the network boundary (connect to external networks only through managed interfaces). Configure network devices in accordance with the *Cyber Security Standard – Network Security*.	✔	✔					✔	Network Security
Change Control	Use a documented change control process that includes change documentation, change records, a security review, technical and business approval, and controlled release through separate development/test and production environments	✔	✔		✔	✔	✔	✔	Secure by Design
SDLC	For any code developed as part of an Information Service, follow a documented system development lifecycle (SDLC) process that includes requirements, design, development, testing, and implementation stages that include cyber security testing/reviews. Conduct code reviews for application changes and any high-risk security issues must be remediated prior to deployment to production. Highly sensitive data in non-production environments must be sanitised (data masked, tokenised, or scrambled).	✔	✔		✔	✔	✔	✔	Secure by Design
Approved Email Service	Send and receive Email through a secure email service with content filtering in place.	✔	✔	✔	✔	✔	✔	✔	Secure by Design
Anti-Malware	Install Anti-Virus protection on all Assets, and configure it to scan in real-time, and update daily.	✔		✔	✔	✔	✔	✔	Threat and Vulnerability Management
Endpoint Detect and Respond Agents (EDR)	For workstations and servers delivered to UNSW - Install UNSWIT Endpoint Detection & Response (EDR) agents.			✔	✔				Threat and Vulnerability Management
Vulnerability and Patch Management	Identify any vulnerabilities from a reputable source or using vulnerability scanning. Assess the risk of vulnerabilities and install any required software and firmware updates in a timely manner.	✔	✔	✔	✔	✔	✔	✔	Threat and Vulnerability Management

5.3. Information Resources with a high cyber security risk rating delivered by a non-UNSW entity, must have as a minimum, the following controls:

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Single Sign On	Use UNSW Single-Sign On.	✓	✓		✓	✓	✓	✓	Access Control
Passwords	Authentication services must enforce UNSW password policies or higher	✓	✓	✓	✓	✓	✓	✓	Access Control
Multi-Factor Authentication	Use multi-factor authentication (MFA) for all access.	✓	✓	✓	✓	✓	✓	✓	Access Control
Privileged Access Management / Least Privilege	Ensure access to privileged administrative (sys admin) and elevated business functions is restricted to those with a documented and approved business or technical need. Use separate credentials for privileged administrative functions and normal user functions. Tools with Privileged Access (Sys Admin) must be approved, controlled, and monitored.	✓	✓	✓	✓	✓	✓	✓	Access Control
Remote Access	Use centralised Remote Access Services provided by Cloud Service Provider providing IaaS, PaaS or SaaS, including encrypted VPN and multi-factor authentication (MFA). Restrict remote services to the least functionality required.	✓	✓	✓	✓	✓	✓	✓	Access Control
Segregation of Duties	Segregate access to minimise the occurrence of errors or unauthorised privileged operations.	✓	✓	✓	✓	✓	✓	✓	Access Control
Data and Media Protection	Data protection and associated media protection must be in accordance with the *Cyber Security Standard – Data Security*.	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption at Rest	Encryption must be applied in accordance with the *Cyber Security Standard – Data Security.*	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption in Transit	Encrypt all data in transit outside the network segment or VLAN where Information Asset is located.	✓	✓	✓	✓	✓	✓	✓	Data Security
Encryption Key Management	Manage cryptographic keys in accordance with the *Cyber Security Standard – Data Security*	✓	✓	✓	✓	✓	✓	✓	Data Security
Incident Management	Report cyber security incidents to the UNSW IT Service Desk.	✓	✓	✓	✓	✓	✓	✓	Incident Management

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Asset Inventory	Maintain a centralised inventory (CMDB) and record / register Information Services including ownership, data classification, business impact assessment, risk rating, and location. Update as underlying assets in the service change.	✓	✓	✓	✓	✓	✓	✓	Information Asset Management
Software Asset Management Agents (SAM)	For workstations and servers delivered to UNSW - install UNSWIT Software Asset Management (SAM) agents			✓	✓				Information Asset Management
Business Continuity Plan	Document and annually test a Business Continuity Plan for the service, that addresses loss of location, personnel, technology and any third party required for operation and support of the service.	✓	✓	✓	✓	✓	✓	✓	Information Asset Management
End of Life / End of Support	Do not use end-of-life or end-of-support hardware or software with the Service. Once identified any end-of-life or end-of-support hardware or software must be segmented from the rest of the network.	✓	✓	✓	✓	✓	✓	✓	Information Asset Management
Security Documentation	Develop a service management plan/service handbook that describes system boundaries, system environments, connections with other systems, and what / how security controls are implemented and how they are operated.	✓	✓			✓	✓	✓	Information Asset Management
Physical and Environmental Controls	Use an approved Data Centre, Cloud Service, or ensure compliant physical and environmental controls are in place.	✓	✓	✓	✓	✓	✓	✓	IT Hosting
Security Event Logging	Log all required security events to the complying Centralised SIEM of the service provider of any managed service/cloud service. Synchronise internal system clocks with an authoritative (IaaS Vendor, or Government) time source.	✓	✓	✓	✓	✓	✓	✓	Logging and Monitoring
Security Event Monitoring	Utilise a compliant Managed Service Provider (or the service provider of any managed service/ cloud service), to monitor logs in SIEM.	✓	✓	✓	✓	✓	✓	✓	Logging and Monitoring

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Denial of Service	Ensure Denial of Service (DoS) protection is included in hosting, logging capacity is sufficient to meet Standards, and service resilience meets RTO / RPO.	✓	✓					✓	Network Security
Network Intrusion Detection	Monitor network traffic for anomalous and potentially suspicious data transfers. Networks must include IDS/IPS agents with monitoring by a central SOC.	✓	✓					✓	Network Security
Network Security	Install a firewall at the network boundary (connect to external networks only through managed interfaces). Configure network devices in accordance with the *Cyber Security Standard - Network Security.*	✓	✓					✓	Network Security
Network Segmentation	Implement subnetworks for workloads with different risks/functions. Only allow access from explicitly defines domains, or IP addresses.	✓	✓		✓	✓	✓	✓	Network Security
Networks - Wireless	Wireless access must be authenticated, encrypted, and connected to SIEM and intrusion detection systems are implemented to identify rogue wireless devices and compromises.	✓	✓						Network Security
Web Application Firewall	Use a Web Application Firewall (WAF) in front of all externally facing Information Services.	✓	✓			✓	✓	✓	Network Security
Baseline Configuration	Use a compliant baseline configuration provided by a Cloud Service Provider (CSP) or research partner.	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Change Control	Use a documented change control process that includes change documentation, change records, a security review (for high risk), technical and business approval, and controlled release through separate development/test and production environments.	✓	✓		✓	✓	✓	✓	Secure by Design
Enterprise Security Architecture	For Information Services - Use security architecture, designs, and specifications that are consistent with the Enterprise Security Architecture (ESA) and accurately and completely describe compliant security functionality.	✓	✓	✓	✓	✓	✓	✓	Secure by Design

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
SDLC	For any code developed as part of an Information Service, follow a documented system development lifecycle (SDLC) process that includes requirements, design, development, testing, and implementation stages that include cyber security testing/reviews. Conduct code reviews for application changes and any high-risk security issues must be remediated prior to deployment to production. Highly sensitive data in non-production environments must be sanitised (data masked, tokenised, or scrambled).	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Approved Email Service	Send and receive Email through a secure email service with content filtering in place.	✓	✓	✓	✓	✓	✓	✓	Secure by Design
Backup and Recovery	Create and securely store backups based on business system owner agreed backup cycles (daily, weekly, monthly). Encrypt backups where required. Establish immutable backup (fixed, unchangeable and can never be deleted) where required. Conduct periodic restoration testing.	✓	✓	✓	✓	✓	✓	✓	Secure Continuity
Disaster Recovery Plan	Establish compliant Disaster Recovery infrastructure (for all services other than with recovery time objective (RTO) and recovery point objective (RPO) consistent with those required for business continuity. Document and test-related Disaster Recovery Plans on at least an annual basis.	✓	✓		✓	✓	✓	✓	Secure Continuity
Anti-Malware	Install Anti-Virus protection on all Assets, and configure it to scan in real-time, and update daily.			✓	✓	✓	✓	✓	Threat and Vulnerability Management
Endpoint Detect and Respond Agents (EDR)	Install Endpoint Detection & Response (EDR) agents on all workstations and servers. For workstations and servers delivered to UNSW - Install UNSWIT Endpoint Detection & Response (EDR) agents.	✓	✓	✓	✓	✓	✓	✓	Threat and Vulnerability Management

Control	What to Do	Applications, including SaaS	Networks and Network Devices including SDN	Endpoints (Workstations, Laptops, Mobile Devices, IoT and VDI including BYOD)	Servers Server Instances, including VM, IaaS, PaaS, Containers, and Serverless)	Data and Storage Services, including PaaS	Cyber Security Services, including PaaS and SaaS	Hosting Platforms, including ESX Hosts, Data Centres, IaaS, and PaaS	Where to go for further information
Penetration Testing	Conduct independent penetration testing annually and with any subsequent significant change, for any externally facing service. Remediate findings in a timely manner.	✓	✓		✓	✓	✓	✓	Threat and Vulnerability Management
Vulnerability and Patch Management	All vulnerabilities must be identified (from vulnerability scanning or reputable sources) and assessed for risk to the service. Install any required software and firmware updates related to the vulnerabilities in a timely manner and in accordance with the *Cyber Security Standard – Threat and Vulnerability Standard*.	✓	✓	✓	✓	✓	✓	✓	Threat and Vulnerability Management
Vulnerability Scanning	For Information Services - Conduct regular (monthly) vulnerability scanning on high-risk Information Resources with findings recorded in a risk register and actions initiated in a ticketing system.	✓	✓	✓	✓	✓	✓	✓	Threat and Vulnerability Management
Vendor –Regulatory Compliance (Critical Infrastructure)	For Information Services – Where required, comply with legislative requirements to notify data storage and processing services (such as data centre and cloud storage services) providers that their service is used for business-critical data assets and that their service is in turn a 'critical infrastructure asset'.	✓				✓	✓	✓	Vendor Risk Management

6. Control Gap Assessment and Improvement

6.1. Business Owners must satisfy themselves that all Information Resources within their area of accountability comply with the required minimum controls in Sections 4 and 5. This may be performed in consultation with Chief Information Security Officer, or delegate.

6.2. For medium and high cyber risk rated Information Resources within their area of accountability, Business Owners must:

a) report non-compliance to the Chief Information Security Officer or delegate.

b) record control deficiencies.

c) prioritise control improvements based on the cyber security risk rating. The *UNSW Risk Management Framework* must be used for any additional priority granularity required.

d) assign a due date for control improvement activities.

e) allocate, or require the allocation of adequate resources for control improvement.

f) monitor the status of control improvements.

g) obtain assistance as required from the Chief Information Security Officer, or delegate.

7. Management Attestation

7.1. Deans, Head of Schools, Heads of Research Centres, and Heads of Administrative Units must attest to compliance with the Cyber Security Policy Framework in accordance with the *Cyber Security Attestation Guidelines.*

8. Exemptions

8.1. Any exemption or deviation from this Cyber Security Standard must be approved in accordance with the *Cyber Security Standard – Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

9. Appendix A – Cyber Security Risk Rating Criteria

9.1. Information Resources that store, transmit, or process Highly Sensitive data outside the OECD*, or are proposed to be located outside the OECD* must be referred to the Chief Information Security Officer or delegate for risk assessment and cyber security control requirements.

9.2. The cyber security risk rating of other Information Resources must be determined using the highest applicable rating in *Table 1* below. Cyber Security risk ratings have predetermined likelihood and impact to ensure alignment with the *UNSW Risk Management Framework*.

Table 1.

Information Resource (Information Service or Information Asset)	Low Risk Rating	Medium Risk Rating	High Risk Rating
Applications including SaaS and Mobile Apps	Satisfies all the following: (1) Stores, processes, or transmits public, private, or less than 1000 records of sensitive digital information. (2) Does not provide an ongoing UNSW business or technical function. (3) Loss of Confidentiality, Integrity, and Availability (CIA) will result in only minor consequences to UNSW.	Satisfies any of the following (1) Provides an ongoing UNSW business or technical function. (2) Stores, processes, and transmits 1000-10000 records of sensitive digital information AND stores, processes, and transmits less than 1000 records of highly sensitive digital information And satisfies none of the criteria for high risk	Satisfies any of the following: (1) Stores, processes, or transmits 10,000 or more records of sensitive digital information. (2) Stores, processes, or transmits 1000 or more records of highly sensitive digital information (3) Cannot sustain > 24hr outage (4) Has a business requirement, external partner, or regulatory requirement for high security (5) provides a security service or safety function

Information Resource (Information Service or Information Asset)	Low Risk Rating	Medium Risk Rating	High Risk Rating
Endpoints (including Workstations, Laptops, Mobile Devices, IoT and VDI)	Satisfies all the following: (1) Is NOT publicly accessible (2) Is in an isolated network or standalone with no access to the UNSW network, (3) Stores, processes or transmits public, private or less than 1000 records of sensitive digital information	Satisfies any of the following (1) Is publicly accessible (2) Is connected to the UNSW network (3) Stores, processes, and transmits 1000 or more records of sensitive digital information AND stores, processes, and transmits less than 1000 records of highly sensitive digital information And satisfies none of the criteria for high risk	Satisfies any of the following: (1) Stores, processes, or transmit 1000 or more records of highly sensitive digital information (2) Cannot sustain > 24hr outage (3) Used for system administration of a high-risk application or Information Service (4) Has a business requirement, external partner or regulatory requirement for high security
Server instances (including virtual machines, IaaS and PaaS (including containers and serverless))	Server supports only low-risk applications or Information Services	Server supports medium-risk applications or Information Services	Server supports any high-risk applications or Information Services or security service
Data Services and Storage Services (including PaaS)	Data Service or Storage supports only low risk applications or Information Services	Data Service or Storage supports medium-risk applications or Information Services	Data Service or Storage supports any high-risk applications or Information Services, or security service
Hosting Platforms (including ESX hosts, data centres, IaaS, and PaaS)	Hosting platform supports only low-risk applications or Information Services	Hosting platform supports medium-risk applications or Information Services	Hosting platform supports any high-risk applications or Information Services, or security service
Networks and Network Devices (including SDN and Cloud)	Network or Network device supports only low risk applications or Information Services	Network or network device supports medium-risk applications or Information Services	Network or network device supports any high-risk applications or Information Services, or provides a security service
Cyber Security Services including SaaS and PaaS	Security Service supports only low-risk applications or Information Services	N/A	Security Service supports any medium or high-risk applications or Services

* Organisation for Economic Co-operation and Development (OECD) member countries.

9.3. Where the Cyber Security risk rating cannot be assessed using the table above, it can be assessed using the equivalent impact rating in the *UNSW Risk Management Framework*.

Cyber Security Risk Rating	Low Risk Rating	Medium Risk Rating	High Risk Rating
Equivalent Inherent Risk Impact rating from UNSW Risk Management Framework.	Impact: Insignificant	Impact: Medium and Substantial	Impact: Major and Severe

Accountabilities	
Responsible Officer	Chief Information Security Officer
Contact Officer	Head of Cyber Security Governance and Strategy
Supporting Information	
Legislative Compliance	Privacy and Personal Information Protection Act 1998 (NSW) Security of Critical Infrastructure Act 2018 Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
Parent Document (Policy)	Cyber Security Policy
Supporting Documents	UNSW Data Classification Standard Cyber Security Standard - Data Security Cyber Security Standard - Vendor Risk Management Cyber Security Standard - Access Control Cyber Security Standard - Incident Management Cyber Security Standard - Logging and Monitoring Cyber Security Standard - IT Hosting Cyber Security Standard - Secure Continuity Cyber Security Standard - Threat and Vulnerability Management Cyber Security Standard - Network Security Cyber Security Standard – Information Asset Management Cyber Security Standard - Secure-By-Design Cyber Security Attestation Guidelines
Related Documents	Acceptable Use of Information Resources Policy Cyber Security Standard – End User Computing UNSW Risk Management Framework UNSW Enterprise Risk Criteria and Categories UNSW Business Continuity and Resilience Framework 2021v11
Superseded Documents	ITSS-17 IT Security Standard – Information Security Risk and Compliance Management, v1.0
File Number	[For Governance Use]
Definitions and Acronyms	
Area of Accountability	Any area where a person has strategic, structural, operational, or financial control over any Information resources within that area.
Business Owner	Means a person with primary accountability for the business or technology functions provided by one or more UNSW Information Resources, including any associated cyber security. Note: The Business Owner of an Information Service may be located in the UNSWIT unit or any other organisational unit.
CIA (Confidentiality, Integrity, and Availability)	**Confidentiality -** Preserving authorised restrictions on access and disclosure, including means for protecting UNSW information. **Integrity -** The guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. **Availability -** Ensuring timely and reliable access to and use of information.

Critical asset	Means a UNSW Information Resource that is subject to a contractual or regulatory requirement for central logging and monitoring or has greater than 1,000 records of highly sensitive data, or has greater than 10,000 records of sensitive data, or provides a cyber security function, or is a Server/Data Service/Network Service/Hosting Platform that supports such Information Resources.
Cyber security review	Means audits, reviews and other assurance activities required to meet UNSW cyber security risk management, legislative, compliance, or contractual requirements.
Cyber security risk	Means the risk of a cyber security event or incident.
Digital information	Means information that is in a digital or electronic form and is stored, processed or transmitted within an Information Service or Information Asset.
EDR	Means Endpoint Detection and Response - a solution that records and stores endpoint-system-level behaviours, uses various data analytics techniques to detect suspicious system behaviour, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems.
External Party	Means any external entity or a person that is not part of the UNSW. Examples include vendors and suppliers, customers, regulatory bodies, other universities, and collaborative partners.
Information Asset	Means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that stores, processes or transmits UNSW digital information.
Information Asset Owner	Means the person who is accountable for the day-to-day operation and protection of an Information asset.
Information Resource	Means any Information service, Information asset or digital information.
Information Service	Means any business or technology function using one or more Information assets including but not limited to: (a) application systems (including software-as-a-service); and (b) IT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.
Information Service Owner	Means the person responsible for defining, operating, measuring, and improving an Information service and associated cyber security controls. Also known as “System Owner”.
Inherent Risk	Means the risk level or exposure of an Information Resource without taking into account the actions (e.g., controls) that the UNSW has taken or might take. Inherent risk is determined based on criteria defined in the *Cyber Security Standard – Risk Management*.
Recovery Point Objectives	Point to which digital information used by an activity must be restored to enable the activity to operate on resumption. Also be referred to as “maximum data loss”.
Recovery Time Objectives	Time goal for the restoration and recovery of functions or resources based on the acceptable downtime and acceptable level of performance in case of a disruption of operations.
Significant Change	Any change to a system’s configuration, environment, information content, functionality, or users which is identified as a High-risk change as per the Risk Assessment for Change Type.
UNSW Entity	Means a university-owned, controlled, or fully managed entity, Examples include but are not limited to Business Units, faculties, divisions etc.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
#.#	[to be completed]	[to be completed]	[to be completed]	[to be completed]