UNSW College

# IT Security Policy

## 1. Purpose

UNSW College acknowledges that the use of Information and Communication Technology (ICT) is crucial in supporting the range of professional services it delivers.

The objective of this Policy is to:

(a) provide a framework for managing the security of UNSW College ICT systems and information assets;

(b) assist the College to ensure the accuracy, confidentiality, integrity and availability of ICT systems and information assets;

(c) provide supporting controls relating to data handling practices outlined in the Data Governance Policy and Privacy Policy; and

(d) identify the roles, responsibilities and accountability of users and providers of ICT systems and information assets.

The College aims to manage information security risks using a risk-based approach aligned to the Risk Management Framework Policy.

## 2. Scope

This Policy applies to:

(a) the management of all information security matters at the College;

(b) all College ICT systems and information assets regardless of location; and

(c) all Users of College ICT systems and information assets.

In addition, the UNSW Cyber Security Policy and Standards apply to all Users of UNSW ICT information systems and information assets. UNSW Policies are publicly available on its Governance website: www.unsw.edu.au/governance/policy.

## 3. Policy statement

### 3.1 Data backup

(a) The College recognises that Backup of important information is often the last line of defence in the event of either accidental or malicious loss or modification of the College's information, applications and infrastructure configurations.

(b) Information held and managed by the College is backed up on a regular basis, and protected from Unauthorised Access or Modification, so the information is available to be recovered in a timely manner.

### 3.2 Data security

(a) The College acknowledges that appropriate data security controls reduce the likelihood (and impact) of data breach incidents during various phases of the data lifecycle.

(b) The College uses security technology solutions in line with the UNSW Cyber Security Standard – Data Security.

### 3.3 Cyber security incident management

(a) The College recognises that Cyber Security Incidents can originate from intentional or unintentional actions. Outcomes of a Cyber Security Incident may include financial detriment, loss of data including Personal Information, impacts to third parties, regulatory sanctions, lack of ICT resource availability and reputational loss to the College.

(b) The College operates security controls in order to reduce the likelihood and impact of Cyber Security Incidents.

(c) All College staff are required to comply with the Acceptable Use of ICT Resources Policy (Staff), which helps to mitigate the risk of Cyber Security Incidents.

(d) Where technically possible, the detection and reporting of potential Cyber Security Incidents must be automated.

(e) Potential Cyber Security Incidents must be immediately reported to the Head of IT and the Head of Legal and Compliance in the first instance.

### 3.4 Security vulnerability management

(a) The College acknowledges that managing Security Vulnerabilities on operating systems, applications and devices is a critical activity in ensuring the security of College ICT systems and information.

(b) The IT department is responsible for maintaining standard security configurations for all systems in line with the recommendations of its ICT vendors. This includes actively scanning and reviewing systems for vulnerabilities.

### 3.5 User access management

(a) The College recognises that Unauthorised Access or Modification to ICT systems could enable a malicious or accidental security breach that could lead to unwanted release or manipulation of data, Personal Information or Sensitive Information, potentially resulting in productivity, reputational or financial loss to the College or cause serious harm to individuals to whom the data relates.

(b) The College applies access control practices to protect its information and systems from Unauthorised Access or Modification, disclosure or destruction, and to ensure that information remains accurate, confidential, and is available when required.

(c) UNSW College carries out periodic user access reviews for critical systems.

(d) Passwords are mandatory for all User accounts on all networked and stand alone ICT systems including operating systems, applications, databases, End User Computing hardware and mobile devices.

(e) All Users are personally responsible for the use of their account and for the safety and security of their passwords.

### 3.6 Identity and Access Management

(a) All employees and contractors accessing corporate applications and resources on behalf of UNSW College must use Azure Active Directory single sign-on to authenticate and access these resources. This includes 3rd-party applications and solutions which are not necessarily maintained by UNSW College IT i.e. Internet-based Software as a Service (SaaS) solutions.

(b) Azure AD single sign-on will be the standard authentication method for all corporate applications and resources, and all new applications and resources must be configured to use Azure AD single sign-on (SSO). This is to ensure that access to UNSW College data is secure, compliant with regulatory standards, and aligned with organisational policies.

(c) Where Azure AD single sign-on is not available to configure, UNSW College IT, and Legal and Compliance must be engaged in order to provide a sufficiently secure solution.

(d) Exceptions to this policy must be approved by the Head of IT.

### 3.7 Security events logging and monitoring

(a) The College acknowledges that the detection of potential or actual Cyber Security Incidents relies on timely and comprehensive event information being available from key security controls.

(b) The IT department is responsible for logging data relating to activity and security events on network, computer and storage devices including ICT Systems and applications.

### 3.8 Cloud computing security

(a) The College acknowledges that a security breach targeting Cloud Service Providers (CSP) can significantly damage the College's reputation.

(b) It is the College's Policy to consider the risk to information that will be created, stored, transmitted or processed within a cloud-based service. The IT department is responsible for deploying appropriate measures to manage these risks to an acceptable level.

(c) Any person engaging a CSP on behalf of the College must ensure that the contractual requirements with the CSP meet the College's IT Policy requirements (as amended from time to time) and regulatory requirements. All procurement processes must adhere to the Procurement Policy.

(d) Third party risk is further detailed in Section 3.19 below.

### 3.9 Change management

(a) The College recognises that the ICT Change Management process ensures the stability and availability of related ICT systems across the College. This is managed via the IT Change Management Procedure.

(b) Any change to production ICT systems must first be logged and approved through the Change Approval Board (CAB).

### 3.10 ICT system acquisition and development

(a) The College acknowledges that ICT systems are susceptible to attack and therefore security controls must be embedded throughout the application lifecycle.

(b) ICT security requirements must be addressed within the application lifecycle, to reduce the risk of vulnerabilities being introduced during the acquisition or development of new ICT systems.

### 3.11 Web application security

(a) The College acknowledges that web applications represent one of the highest exposures to security attacks and as such need to be designed, built and tested (verified) to ensure that security is applied at all layers of the application and technology.

(b) Assessment and design guidelines provide controls which must be followed when developing internet facing (Web) applications.

(c) All Web applications must continue to be monitored for data breaches. In the case of data breach, the IT team must respond immediately to isolate the affected services and subsequently contact the Head of Legal and Compliance to initiate any requirements pursuant to the Data Breach Response Procedure.

(d) Any compromised service must be fully forensically investigated to determine whether a data breach has occurred.

### 3.12 Physical security

(a) The College acknowledges that critical ICT systems and information assets must be protected from physical theft or environmental damage (such as fire or water damage).

(b) All staff, contractors, vendors and visitors must be authorised by an appropriate approval authority for physical entry into secure College facilities.

(c) All data centre facilities must be equipped with environmental controls to manage environment threats such as water, power or temperature, and other threats known or likely to occur at their geographical locations.

(d) All equipment utilities (e.g. UPS, generator, fire suppression system) must be monitored in accordance with manufacturer specification and correctly maintained.

### 3.13 Bring Your Own Device (BYOD) Policy

(a) The College recognises that its BYOD Policy provides choice and flexibility for staff and students, but also necessitates additional security controls and measures to protect College information and systems.

(b) Users connecting personally owned devices to College networks must comply with secure practices to ensure the security of College networks and data in their devices.

(c) The College will monitor device usage in line with the Acceptable Use of ICT Resources Policy, privacy law and the Workplace Surveillance Act 2005 (NSW). Such surveillance may be undertaken by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of internet websites).

(d) The College reserves the right to disconnect any device that places the College ICT environment at risk.

### 3.14 End user protection

(a) The College recognises that End User Computing hardware (e.g. desktop, notebook workstations or tablets) are the primary gateway to the organisation's sensitive information, confidential information and business applications. Consequently, end user protection is critical to ensuring a robust, reliable and secure ICT environment. Failing to use end user protection can result in an Information Security Incident, causing financial and/or reputational loss to the College.

(b) The College applies security mechanisms, such as operating level security, application level security and computing security, to prevent the unauthorised disclosure and/or modification of College data.

### 3.15 Network security

(a) The security of College data in private and public networks is mostly managed by UNSW IT. Where it is managed by the College, this Policy and the associated IT Policy and Procedure framework applies.

(b) UNSW network architecture and the controls which are applied to ensure the security of data are outlined in UNSW's Cyber Security Standard – Network Security.

### 3.16 ICT recovery

(a) The College recognises that service availability is critical for College ICT communications, infrastructure, systems and applications and as such, a Business Continuity Plan (BCP) and supporting processes must be in place to enable the recovery of business-critical College services.

(b) The BCP must enable appropriate recovery strategies to restore business functions in the required time following any disruption of service or disaster through an appropriate combination of ICT process workaround procedures, technical redundancy and ICT recovery planning.

### 3.17 Information security risk and compliance management

(a) The College recognises that risk management is at the core of the Information Security Management System and as such, information security risk must be identified, mitigated and monitored through a formalised risk management process.

### 3.18 Human resources security

(a) Human Resources will facilitate access for individual employees to the College's ICT systems.

(b) Line leaders and Human Resources must ensure that all College staff or any other Users engaged by College personnel complete the College's ICT security processes particularly when commencing or ceasing their employment or engagement at the College. This includes completing the IT Induction for College staff prior to commencing access to ICT systems.

### 3.19 Acceptable use of ICT

(a) All Users who have access to the College's ICT systems and services must adhere to specific rules regarding use of the College's ICT resources, and their use of the internet, email and social media. These rules are specified in the Acceptable Use of ICT Resources Policy documents for staff and students.

### 3.20 Awareness and Training

UNSW College shall ensure that users are made aware of the Information Security risks associated with their roles and that users understand their obligations and the applicable laws, policies, standards and procedures related to the security of systems and information.

### 3.21 Third party risk management

(a) Users (regardless of location) must not store information assets on the ICT systems of external providers, unless use of the facility has been approved by the applicable asset owner and the Head of IT.

(b) An evaluation process must be undertaken to assess the suitability of external providers who will provide ICT services to the College, share data or otherwise become Users of the College's systems. The considerations for this evaluation are outlined in UNSW's Cyber Security Standard - Vendor Risk Management.

(c) No external provider may commence handling or processing any information assets for the College until it has entered into an appropriate contract with the College that includes relevant information security controls with which the provider must comply. This contract may include a data sharing arrangement where relevant.

(d) External providers must adhere to the College's ICT requirements, including this Policy and any other Policies or Procedures relating to handling of data such as the Privacy Policy and the Data Governance Policy. The Data Classification Standard outlines the minimum level of protection necessary for each classification of data.

(e) Without limiting external providers' other obligations set out in this Policy, external providers must implement, operate and maintain the appropriate information security controls as specified in their contracts with the College.

(f) The College Executive team are responsible for ensuring that external providers engaged by each function are monitored and reviewed for ICT risks, and for managing changes to external provider contracts, taking into account information assets and information systems.

(g) External providers must ensure that they only connect devices to the College network using approved secure access methods.

(h) External providers accessing confidential information must enter into a Confidentiality Agreement before receiving access to that information.

(i) UNSW data may only be made available to third parties by the College where UNSW has authorised that disclosure. Such data must be used in accordance with UNSW's requirements.

## 4. Breaches and non-compliance

### 4.1 Any breach of this Policy or related processes may result in:

(a) suspension of access to the ICT system or information asset, or other systems;

(b) disciplining action as available to the College, and/or;

(c) termination of contract and/or further legal action;

External providers who breach this Policy may be subject to suspension of access, termination of contract and/or further legal action.

### 4.2 Notification of breaches and non-compliance

(a) Users must promptly report potential breaches of this Policy and suspected information security weaknesses to the Head of IT.

(b) Users must notify the Head of IT and the Privacy Officer immediately of any potential data breach in accordance with the Data Breach Response Procedure.

(c) Anyone who identifies any damage to, or loss of, College or UNSW server or network hardware or software must promptly report this to the Head of IT.

(d) Asset owners and service owners are responsible for ensuring that faults with business-critical applications are reported to the Head of IT as quickly as possible.

## 5. Roles, responsibilities and delegations

| Role | Responsibility |
|---|---|
| Head of IT | Implementing, disseminating and reviewing this Policy. |
| IT Operations Manager | The day to day implementation of this Policy and being the first point of contact for enquiries. |
| Manager IT Solutions | Assisting the Head of IT to implement this Policy. |

## 6. Definitions

| Definitions and Acronyms | |
|---|---|
| Backup | Copying and archiving of computer data so it may be used to restore the original after a data loss event. |
| Business Continuity Plan | A plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency. |
| Change Management | An IT service management discipline, which ensures that changes to services and configuration items are documented, approved and implemented in a planned and controlled manner. |
| Cloud Service | Any service made available to Users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on premises servers. |
| Cloud Service Providers (CSPs) | Third parties that provide Cloud Services to the College under a written agreement. |
| Confidential information | Includes, but is not limited to, any trade or business secrets, customer or client details and lists, supplier details and lists, the identity and source of the College's suppliers, pricing information, marketing information, strategic information, financial information, and any other information that a reasonable person would know to be confidential or sensitive to the business of the College. |
| Cyber Security Incident | An act of denying, disrupting or stealing of information on ICT systems. |
| Data | The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Data is typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not Information until it is used in a particular context for a particular purpose. Data is typically considered to be conceptually at the lowest level of abstraction. |
| Data held in a computer | Data held in any removable data storage device for the time being held in a computer, or data held in a data storage device on a computer network of which the computer forms a part. |
| End User Computing (EUC) | Using a computer at the application level. The term end user is used to distinguish the person for whom the product was designed from the person who programs, services or installs the product. |
| External provider | An external entity or person that provides an ICT system to the College or a service that involves the handling or processing of information assets. |
| ICT System | Hardware, software, devices, networks, media and other resources that store, process or transmit information assets, whether individually or in combination. |
| Information asset | Recorded information in any format and may include data, personal information and confidential information. |

| | |
|---|---|
| Information security | The preservation of the confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability of information assets. |
| Information Security Incident | A warning that there may be a threat to information or computer security. |
| Integrity | Means that information assets, facilities and services are what they are reasonably represented as, and are protected from tampering which would make their content or |
| Modification | In respect of data held in a computer, means the alteration or removal of the data or an addition to the data. |
| Personal Information | As defined in the *Privacy Act 1988* (Cth), means information or an opinion about an identified individual, or an individual who is reasonably identifiable:<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not.<br>Examples of Personal Information include:<br>(a) a record which includes an individual's name, address, date of birth, mobile phone number or email address;<br>(b) photographs, images, video or audio footage of an individual;<br>(c) the fingerprints, blood or DNA samples of an individual. |
| Security Event | A change in the everyday operations of a network or information technology service indicating that a security Policy may have been violated or a security safeguard may have failed. |
| Security Vulnerability | A weakness in a product, in particular computer software, that could allow an attacker to compromise the integrity, availability or confidentiality of that product. |
| Sensitive Information | Defined in section 6 of the Privacy Act 1988 (Cth) to mean:<br>(a) information or an opinion about an individual's:<br>i. racial or ethnic origin;<br>ii. political opinions;<br>iii. membership of a political association;<br>iv. religious beliefs or affiliations;<br>v. philosophical beliefs;<br>vi. membership of a professional or trade association;<br>vii. membership of a trade union;<br>viii. sexual orientation or practices; or<br>ix. criminal record;<br>(b) that is also Personal Information;<br>(c) health Information about an individual;<br>(d) genetic information about an individual that is not otherwise health information;<br>(e) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or<br>(f) biometric templates. |
| Surveillance | Surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer |

| | |
|---|---|
| | (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites), as defined by the *Workplace Surveillance Act 2005* (NSW). |
| Unauthorised Access or Modification | (a) access to data held in a computer;<br>(b) modification of data held in a computer;<br>(c) the impairment of electronic communication to or from a computer; or<br>(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;<br>(e) by a person who is not entitled to that access, modification or impairment. |
| UPS | An Uninterruptible Power Supply or Uninterruptible Power Source, being an electrical apparatus that provides emergency power to a load when the input power source or mains power fails. |
| User | Any person who uses, or may impact the security of, College information assets and ICT systems over whose activity the College may reasonably expect to able to exert authority. This includes, but is not limited to UNSW and College staff (including casuals), contractors, students and other third parties such as external providers, consultants, agents and agency staff. |

| Related Policy Documents and Supporting Documents | |
|---|---|
| Legislation | • Workplace Surveillance Act 2005 (NSW)<br>• Privacy Act 1988 (Cth)<br>• Cybercrime Act 2001 (Cth)<br>• General Data Protection Regulation (EU) 2016/679, where applicable<br>• UK GDPR, being the General Data Protection Regulation (EU) as amended and incorporated into law in the United Kingdom<br>• Spam Act 2003 (Cth)<br>• State Records Act 1998 (NSW) |
| Policy | • Acceptable Use of ICT Resources Policy (Staff)<br>• Acceptable Use of ICT Resources (Students)<br>• Privacy Policy<br>• Data Governance Policy<br>• Data Classification Standard<br>• Mobile Devices Policy<br>• Risk Management Framework Policy<br>• IT Induction for College staff<br>• Procurement Policy<br>• UNSW Cyber Security Policy and Standards (such as the Cyber Security Standard – Vendor Risk Management) - available at www.unsw.edu.au/governance/policy)<br>• UNSW Data Classification Policy and Standard<br>• UNSW Data Governance Policy and Standard<br>• UNSW Recordkeeping Policy and Standard |

| | |
|---|---|
| | • UNSW Privacy Policy |
| Procedures | • IT Asset Management Procedure<br>• IT Change Management Procedure<br>• Data Breach Response Procedure |

**Policy Governance**

| IT Security Policy | |
|---|---|
| Category/Business Group | Information Technology |
| Published Externally (Yes/No) | Yes |
| Approver | Chief Executive Officer |
| Responsible Officer | Chief of Staff |
| Contact Officer | Head of Information Technology |
| Effective Date | 17/08/2023 |
| Next Review Date | 17/08/2026 |
| Version | 1.0 |

**Revision History**

| Version | Approved by | Approval date | Effective date | Sections modified |
|---|---|---|---|---|
| 3.0 | Sarah Lightfoot, CEO | 11 August 2023 | 17 August 2023 | Reviewed and updates made as per Cyber security current state review, including:<br>• New section 3.6<br>• New section 3.20<br>• Updating references to UNSW Security Standards<br>• Administrative updates<br>• Updating all references from 'UNSW Global' to 'UNSW College' and updating Policy template to reflect the new UNSW College brand guideline<br>• Cosmetic changes applied across the document to ensure consistency with other policies |
| 2.0 | Laurie Pearcey, CEO | 25/09/2020 | 25/09/2020 | Alignment of terms with the Data Governance Policy and other administrative and procedural updates |
| 1.0 | Rob Farage, CEO | 01/10/2017 | 01/10/2017 | N/A |

Please visit our website to ensure that you have the latest version of this Policy. Policies are available at: unswcollege.edu.au/about/policies