Charles Sturt University

Information Security Guidelines appendices

Appendix A – Information security documentation framework

This document establishes the minimum objectives for effectively protecting the University's information and its respective information assets. It consists of high level statements that clearly define the expectations across the University for the protection of information.

This document defines the business and security goals that the University has mandated however it does not mandate how these goals are implemented. Details and guidance on how these goals are implemented are described in supporting documents including, but not limited to, standards and procedure documents.

The information security document contains:

1. policy controls – defines the security requirements necessary to ensure that University information assets are configured and managed in a manner which protects the confidentiality, integrity and availability of the information assets, inclusive of the information hosted on them. Policy controls also define the baseline level of information security requirements within the University which must be adhered to.
2. processes and procedures – descriptions of activities and/or methods to achieve compliance with the Information and Communications Technology Security Policy.
3. technical security standards – defines how the University implements the requirements of policies on various information assets responsible for managing the University's information. These documents support policies in defining detailed security controls within the University environment such as:
    1. Firewall/Router Configuration Standard, and
    2. Secure Configuration and Build Standard.
4. configuration standards – should be in place for all critical system components. The University should ensure that the standards:
    1. address all known security vulnerabilities
    2. are updated as new vulnerability issues are identified, and
    3. are consistent with industry-accepted system hardening standards.
5. all new systems and/or devices – must be based on system configuration standards. Sources of industry-accepted system hardening standards may include, but are not limited to, those from the:
    1. Centre for Internet Security (CIS)
    2. International Organisation for Standardisation (ISO)

3. SysAdmin Audit Network Security (SANS) Institute, and
4. National Institute of Standards Technology (NIST).

6. system configuration standards for all types of system components – should include, but are not be limited to the:
    1. changing of all vendor-supplied defaults and elimination of unnecessary default accounts;
    2. implementation of only one primary function per server to prevent functions that require different security levels from co-existing on the same server
    3. enabling only of necessary services, protocols and daemons as required for the function of the system
    4. implementation of additional security features for any required services, protocols or daemons that are insecure
    5. configuring of system security parameters to prevent misuse, and
    6. removal of all unnecessary functionality such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.
7. security guidelines – contain information that is helpful in executing standards and procedures or implementing technical standards. Guidelines are based on vendor and/or leading practices are non-binding and contain only recommendations.

Appendix B – Risk management

There must be clear direction provided to identify, assess and manage information security risks against criteria for risk acceptance inclusive of objectives relevant to the University. The University is required to adopt a risk-based approach to the application of security measures to protect information.

Information security risk management must be undertaken in compliance with the Risk Management Policy and follow the methodology.

The Division of Information Technology responsibilities include, but are not limited to:

1. defining of security requirements for information assets (e.g. processes, information, applications, and resources)
2. designation of custodians for information assets
3. risk assessment of information assets
4. ensuring the protection of information assets in accordance with Information Security Policies and Procedures
5. development and implementation of Information and Communication Technology (ICT) systems consistent with the security standards for the secure operation of ICT resources
6. provisioning of secure services to agreed service levels with adequate capacity, resilience and contingency
7. coordination, development and distribution of information security policies and procedures
8. monitoring and analysis of security alerts inclusive of the distribution of information to appropriate information security and business departments
9. creation and distribution of security incident response and escalation procedures
10. administration of user accounts and related authentication management
11. monitoring and controlling of access to University data
12. development and implementation of an information security awareness program
13. ensuring that suitable technical, physical and procedural controls are in place in accordance with policies, procedures, and standards and are properly applied and used by all authorised users. Such controls must:
    1. monitor and assess the University's compliance with policy statements, the correct operation of associated controls and their obligations as appropriate
    2. provide oversight of regular information security audits, and
    3. provide and coordinate independent reviews and assessments of internal control systems.
14. ensuring that authorised users:
    1. are informed of their obligations to fulfil relevant corporate policy statements by means of appropriate awareness, training, and education activities upon commencement and on an annual basis, and
    2. comply with procedure and standard statements, actively supporting associated controls.

Specific Division of Information Technology roles and responsibilities may include, but not be limited to:

1. Director, IT Infrastructure and Security:
    1. establish, document and distribute overall strategies for information security

2. provide governance for the implementation of such strategies, and
3. hold accountability for the effectiveness of strategy implementation.

2. Enterprise Architect, Security:
    1. establish, document and distribute security policies and procedures
    2. review implementation and effectiveness of security controls in accordance with defined security policies, and
    3. hold responsibility for the implementation of information security strategies.
3. IT Security Officer:
    1. Monitor and analyse security alerts and information, including but not limited to, unauthorised activity, alerts and/or incidents and/or probable incidents, and
    2. Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
4. Technical Officer:
    1. Monitor and manage user accounts, performing authentication management including, but not limited to, additions, deletions and modifications, and
    2. Implement technical controls as per appropriate to their area of expertise.

Appendix C – Data backup and recovery

To protect against the loss of data in the event of physical disaster or other incident which may lead to the loss of data (e.g. data corruption), the University requires all institutional data to be backed up appropriately.

The purpose of this document is to describe the minimum controls required for data backup regimes to safeguard against the loss of data that may occur due to hardware or software failure, physical disaster or human error.

The University requires all authorised users to be responsible for the management of institutional data and records under their control in accordance with the University's Record Keeping Plan. Authorised users should not rely solely on backup of data to fulfill their responsibilities of record keeping because backups are primarily for the purposes of recovering data in the event of a disaster.

Data backups are not intended to serve as archival copies of data or to meet the University's record keeping and/or retention requirements.

Division of Information Technology is responsible for the backup and recovery of data held in the Institutional Data Centre. However, data custodians are responsible for ensuring that appropriate backup schedules are arranged with Division of Information Technology as appropriate for the data for which they are responsible.

The responsibility for backing up data held outside the University's Data Centre on any computer or device, regardless of whether owned privately or by the University, falls entirely on the authorised user.

Authorised users should consult the IT Service Desk about backup procedures for such computers or devices.

The University requires that all institutional data is backed up according to the following rules:

1. records must be kept of what data is backed up and where it is backed up
2. backup schedules must be maintained
3. backup media must be clearly labelled
4. backups should be stored at a geographically diverse location from the primary location of the data
5. recovery procedures for the restoration of data must be kept up to date
6. six monthly testing of recovery procedures (restoring data from backup copies) must be undertaken to ensure that they can be relied on in an emergency or disaster situation, and
7. records of all the above must be kept for audit purposes.

The University requires that all institutional data is backed up according to the following schedules:

1. backup of structured data (application data and databases)
    1. every day a data backup is taken and retained for 30 days, and
    2. the following schedule provides for data to be restored with at most one working days data missing.

Granularity (length of time between copies)	Retention (length of time the backup copy is kept)	Location (location of backup copy)
12 hours	7 days	Secondary Data Centre
1 week	30 days	Secondary Data Centre
1 month	3 years (7 years for long term retention)	Third off site repository

2. backup of unstructured data (email and documents stored in electronic files)
    1. this schedule is required to protect against accidental deletion of files that could go unnoticed for more than two weeks (e.g. staff and student documents, emails and lecture recordings)

Granularity (length of time between copies)	**Retention (length of time the backup copy is kept)**	**Location (location of backup copy)**
1 day	7 days	Secondary Data Centre
1 week	30 days	Secondary Data Centre
1 month	3 years (7 years for long term retention)	Third off site repository

Document history

Approval date	Resolution or delegation	Nature of Amendment
April 2022		These appendices were previously included in the body of the Information Security Guidelines.