INFORMATION TECHNOLOGY SECURITY POLICY

10 December 2018

Policy No:	DFA.011.18
Adopted by Council:	18/12/2018
Review Date:	December 2020
Responsible Officer:	Director Finance and Administration
Responsible Director:	Director Finance and Administration
Functional Area:	Finance and Administration

CONTENTS

PREAMBLE

Junee Shire Council (JSC) values the use of information technology in supporting the mission of the Council.

JSC information, whether managed and residing on JSC resources or held in trust and managed by third parties or business partners, is an important asset that must be protected. Any person or organisation that uses or holds in trust these assets has a responsibility to maintain and safeguard them.

The Council is committed to preserving the confidentiality, integrity, and availability of information regardless of the form it takes - electronic or non-electronic. Improper use of information resources may result in harm to the Council.

PART 1 – OBJECTIVE

To ensure that JSC information can be used when required with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorised disclosure, damage or loss. The policy reinforces the value of data and information to JSC.

PART 2 – POLICY OBJECTIVES

The IT Security Policy sets out management's information security direction. The purpose is to proactively and actively identify, mitigate, monitor and manage information security vulnerabilities, threats and risks in order to protect JSC and its assets, information and data.

PART 3 – SCOPE

This policy applies to all users of JSC ICT resources – including (but not limited to) staff (including casuals), councillors, consultants and contractors, third parties, agency staff and visitors to JSC. This applies to all JSC IT Assets and all devices connected to the JSC network.

PART 4 – POLICY STATEMENTS

4.1 Data Back Up

Data Backups are primarily a preventative measure to protect against loss of data resulting from system failure (disaster or other), virus/malware attack, system or human error.

Backups are an essential control and safeguard to ensure availability of JSC information being stored, processed or transmitted via information technology communication systems.

Statement: Data will be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster.

4.2 Data Security

JSC supports an extensively broad and complex data landscape. Based on appropriate data classification and handling guidelines, this policy and associated standard ensures that appropriate controls are implemented for the confidentiality and integrity of sensitive data.

4.3 Security Incident Management

Provides preventive, corrective and detective measures, ensuring a consistent and effective approach to the management of information security incidents, including communication of events and weaknesses, such as breach of access.

Well designed, understood tools and processes will help contain, preserve (legal / forensic purposes) and limit any damage resulting from a security incident.

Statement: Incident detection mechanisms such as security event logging and antivirus will be implemented for all IT systems. All potential security incidents must be handled appropriately following a formalised security incident handling process.

4.4 Vulnerability Management

All systems are susceptible to vulnerability (weakness) and therefore under constant threat from malicious exploitation that may result in the compromise of confidentiality, integrity or availability of JSC information or systems, potentially resulting in productivity, reputational or financial loss.

Vulnerability management involves alerting and responding to identified and potential violations or security threats in a timely, measured and prioritised (risk based) manner, in order to prevent or limit the damage. Vulnerability management is considered a preventive and corrective measure.

Statement: Security patch and vulnerability management processes will be put in place to identify, prioritise and remediate security vulnerabilities on IT assets.

4.5 User Access Management

A preventive measure, ensuring only authorised users are granted access to JSC systems. Unauthorised access could enable a malicious or accidental security breach.

Breach of access could lead to unwanted release or manipulation (Integrity) of sensitive information potentially resulting in productivity, reputational or financial loss.

Statement: All user access related requests (e.g. adding new users, updating access privileges, and revoking user access rights) will be logged, assessed and approved in accordance with defined user access management process.

4.6 Logging and Monitoring

Security devices such as firewall, Intrusion detection / prevention, security event incident management, mail content filters and anti-virus all generate log data.

The timely detection of information security incidents relies on comprehensive security log data being available from information technology communication systems.

Statement: Key security-related events such as user privilege changes will be recorded in logs, protected against unauthorised changes and analysed on a regular basis in order to identify potential unauthorised activities and facilitate appropriate follow up action.

4.7 Cloud Security

JSC is increasingly utilising cloud solutions to deliver business solutions and functionality. This Policy and Standard explains what JSC expects of "cloud service providers" to meet security controls and access requirements to ensure all JSC information and system controls are met.

Additionally, cloud service providers have been known to change practices with minimal notice. These impacts need to be managed or mitigated in our agreements to meet JSC service expectations.

Statement: Cloud services used by JSC will be subject to a risk assessment to ensure that the provider of the services has the necessary security controls in place to protect the data of JSC and these risks are managed to an acceptable level.

4.8 IT Asset Management

Asset / Inventory management is key to prudent security and management practices, providing context for all IT Security Policy statements and Standard requirements.

Without an accurate inventory, processes such as vulnerability management are difficult to implement. For example, assessment of in scope devices when responding to critical vulnerabilities, may not be captured, hence devices will remain unpatched and therefore exposed to malicious exploit.

Statement: In the context of this policy, an IT asset is any JSC owned or managed device or service that connects to or is used by JSC in its business activities such as data link, physical device, application (including firmware), database and middleware.

4.9 Change Management

The JSC IT Change Management process ensures stability and availability of related information technology communication systems across JSC. Secure practices including reviews during changes are necessary to ensure service availability.

Statement: Any change to JSC production information systems will be logged and assessed for security and risk impact.

4.10 IT System Acquisition & Development

IT systems (applications, databases & middleware) are susceptible to attack and therefore security controls will be embedded throughout the whole acquisition development lifecycle.

In conjunction with this and other controls, a multi-level approach to information security at each layer of the system will be taken, therefore mitigating the security risk.

Statement: IT security requirements will be addressed to reduce the risk of vulnerabilities being introduced during the acquisition or development of IT systems.

4.11 Web Application Security

Web applications are being used extensively across JSC for the delivery of business services and information. They also represent one of the highest exposures to security attacks. Given the number of security exploits that exist for web interfaces, secure design, implementation and monitoring are essential.

Statement: Web applications need to be designed, built and tested (verified) to ensure security is applied at all layers of the application and technology. Assessment and design guidelines will provide controls to be followed when developing Web applications.

4.12 Physical Security

Physical security is important for critical infrastructure that must be protected from physical (theft) or environmental (fire, water) damage. Physical security is very much a preventive control.

Statement: The facilities (e.g. computer rooms etc.) where critical information is stored or processed, will be constructed and arranged in a way that data is adequately protected from physical and environmental threats.

4.13 Bring Your Own Device (BYOD)

Supporting "Bring Your Own Device" provides choice and flexibility for JSC staff. This allows increased personal productivity and improved work experience but also necessitates additional security controls and measures to protect the JSC information and systems.

This Policy and associated Guideline recognises this need and provides the requirements to manage the risks associated with "BYOD".

Statement: JSC staff, councillors and authorised users connecting personally owned devices to the JSC networks must comply with secure practices to ensure the security of JSC networks and JSC data in their devices.

4.14 End User Protection

JSC end user devices are the primary gateway to JSC's data and business applications. Implementation of appropriate information security controls is necessary to mitigate the risk of inappropriate access to JSC data and IT systems such as malware, information disclosure or loss.

Consequently end user protection is critical to ensuring a robust, reliable and secure IT environment. Failing to do so can result in an information security incident, causing financial and/or reputational loss to JSC.

Statement: End user desktop computers, mobile computers (e.g., laptops, tablets) as well as portable computing devices (e.g. portable hard drives, USB memory sticks etc.) will be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of JSC data.

4.15 Network Security

Network infrastructure and associated data links provide essential connectivity between internal and external systems. In order to provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed in line with current security practises.

Statement: JSC network architecture will be commensurate with current and future business requirements as well as with emerging security threats. Appropriate controls will be established to ensure security of JSC data in private and public networks, and the protection of IT services from unauthorised access.

4.16 IT Recovery

Service availability is critical for JSC Information Technology communications, infrastructure, systems and applications. This Policy ensures that processes are in place to ensure JSC's ability to recover from system and environmental failures, and regular testing of these processes is afforded.

Statement: An IT Recovery Plan and relative process will be in place to enable the recovery of business critical JSC services in a timely manner, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption.

4.17 Information Security Risk & Compliance Management

Risk Management is at the core of the Information Security Management System. Allowing JSC to identify, assess and evaluate risk, enabling, effective management of information security vulnerabilities and threats to its information assets that could adversely affect or provide academic and business opportunities.

Statement: Information security risk will be identified, mitigated and monitored through a formalised risk management process.

4.18 Human Resources Security

Supporting Human Resources policies, the purpose of this Policy and Standard is to define the rules to be followed before, during and after the termination of employment of all JSC employees.

Statement: All JSC staff (Including casuals), consultants, contractors, third parties and agency staff, will be subject to appropriate security processes before, during and after the termination of their employment.

4.19 IT Acceptable Use

JSC embraces and relies on the use of technology, the Internet and digital media to conduct its activities. This Policy and associated Guidelines outline the acceptable practices in the use of technology and access to information sources and systems for JSC system users.

Statement: All users who have access to JSC's IT systems and services must adhere to specific rules regarding use of JSC resources, their internet and email usage as well as when interacting with social media.

4.20 Third Party Risk Management

Outsourced agreements should enforce appropriate information security controls with respect to the nature of the contract i.e. cloud services engagement, to ensure proper due diligence and therefore risk management.

Statement: Security risks arising from JSC contracted third parties (i.e., suppliers, vendors etc.) who maintain direct or indirect access to JSC IT systems and data must be operationally and contractually controlled.

PART 5 – IMPLEMENTATION

The implementation of the IT Security Policy will be achieved by performing an assessment of existing IT Security Practices and the development of suitable guidelines to support the policy.

The appropriate Guidelines supporting the Policy Statements as detailed in Part 4 will be developed over a period of 12 months following adoption of the policy.

PART 6 – REVIEW

The IT Security Policy is an active document and must be subject to review.

This Policy will be reviewed by the Director Finance and Administration every two years from the effective date.

PART 7 – LEGAL & POLICY FRAMEWORK

The IT Security Policy sets the foundation for JSC compliance with:

Digital Information Security Policy (NSW)
State Records Act 1998 (NSW)
Privacy & Personal Information Protection Act 1998 (NSW)
Government Information Classification and Labelling Guidelines 2013 (NSW)
Privacy Amendments (Privacy Alerts) Bill 2013 (Cth)
Privacy Amendment Act 2012 (Cth)
Government Cloud Services Policy and Guidelines (NSW)
Australian Government Protective Security Policy Framework (PSPF)

This policy is aligned with the following JSC internal Policies and protocols:

Business Continuity Plan
Enterprise Risk Management Policy & Framework
Code of Conduct
Records Management Policy
Purchase of Goods and Services

Version Control and Change History

Version	Date	Action
V1.0		Adoption of Policy