Information Security Policy, effective as of 20 February 2020

Information Security Policy

Policy Owner: Chief Executive Officer

Information is an asset, and it needs to be protected from inappropriate modification, loss, disclosure and unavailability. The compromise of any business information could severely impact Infocentric customers, constitute a breach of the law and regulations, and negatively impact the reputation of Infocentric.

The purpose of this policy is to protect information and information systems by mandating a framework of information security controls, management and governance.

Effective information security enables Infocentric to operate competitively, securely and in compliance with laws and regulations across risky and highly regulated environments.

1. Application

This policy applies to all employees and contractors of Infocentric.

This policy also applies to all information owned by Infocentric and information for which Infocentric has responsibility, regardless of whether the information is held on Infocentric property or at other locations.

Infocentric will comply with the minimum standards set out in this policy. In the event a legal obligation imposes a higher standard or requirement on Infocentric, the legal obligation will prevail over the applicable minimum standard.

2. Policy Detail

Policy detail is presented in two parts. First are the information security controls. Second are the information security management and governance processes.

A. Information Security Controls Framework

Background

This information security controls framework describes the information security controls that will be implemented to protect Infocentric information.

Policy statements

1. Security Awareness – To deter insecure behaviour, Infocentric will:

- Educate Infocentric employees, contractors and customers on their accountabilities, responsibilities, and appropriate information security practices.
- Train employees and contractors to fulfil their information security obligations and clear desk requirements.
- Educate Infocentric employees on phishing emails and social engineering to prevent data disclosure.
- Retain attestations of employees and contractors having read this policy.
- Perform background checks on all Infocentric employees.

2. Customer Authentication – To prevent and detect unauthorised processing and repudiation of action, Infocentric will:

- Establish a customer’s identity, associate them with an identifier, and establish terms and conditions before providing any form of access.
- Verify that a person presenting a customer identifier via electronic channels is the same person to whom Infocentric assigned that identifier.
- Manage customer credentials and access to information and information systems.

3. Configuration – To prevent and detect information system vulnerabilities, Infocentric will:

- Determine, implement and maintain the secure configuration of information systems.

4. Cryptography – To prevent loss of security for its most highly classified information Infocentric will:

- Use cryptographic methods to protect information confidentiality and integrity in

5. Information Classification – To prevent and detect loss of information security Infocentric will:

- Identify and classify information and information systems and assign them both owners.

6. Information Handling – To prevent loss of information security while handling information, Infocentric will:

- Prevent unauthorised disclosure of information in accordance with Infocentric will:
- Prevent cryptographic methods from circumventing network perimeter security controls. legal and regulatory requirements.
- Protect information throughout its lifecycle according to its classification.
- Handle information securely, both manually and in information systems.
- Establish non-disclosure agreements before sharing sensitive Infocentric information with external parties.
- Physically protect information and information systems within Infocentric premises.
- Place information systems and network equipment securely.
- Control physical access to Infocentric information on media and in portable devices.
- Control logical access to Infocentric information on media and in portable devices.
- Only handle Infocentric information on personally owned information systems where the end user is subject to and has accepted terms and conditions, and Infocentric information security is protected by approved software.
- Dispose of storage media securely.
- Destroy or not store information in accordance with Infocentric, legal and
- regulatory requirements.

7. Identity and Access Management - To prevent and detect inappropriate access and processing on information systems, Infocentric will:

- Protect information and information systems from unauthorised access.
- Establish the identity of employees, contractors and suppliers prior to providing
- access to information.
- Provide access only when justified by business need, and remove access when
- no longer needed.
- Authenticate access to information systems.
- Hold any person using information systems or accessing information accountable
- for any changes they make.
- Maintain appropriate segregation of duties so that employees and contractors are
- not in a position to perpetrate and conceal unauthorised activities in the normal
- course of their roles.
- Ensure audit trails are enabled, where possible, to capture the following events:
    - User identification
    - Event type
    - Data and time
    - Success or failure indication
    - Origination of event (IP address)
    - Details of affected component or resource
- Audit trails are to be retained for a period of 12 months.

- Ensure that audit trails cannot be altered and that viewing of audit trails is limited to personnel who require access in line with their job role and responsibilities.

8. Information Security Incident Management – To detect and recover from security incidents, and prevent recurrence, Infocentric will:

- Monitor and manage information security events and incidents.
- A security incident is defined as the following:
    - An adverse event or situation associated with the application, infrastructure or related activity that poses a threat to the integrity, confidentiality or availability of the data or information;
    - Any event that could result in loss or damage to the assets;
    - An action that would be in breach of security policies or procedures.

- All incidents are reported and escalated within the Jira Service Desk or to
- *info@infocentric.com.au*
- Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.
- Formal incident reporting and escalation will be implemented.
- To respond to and manage security incidents an Incident Response Team will comprise representatives from different departments to record, assess and remediate. Communication during an incident should be conducted in a manner which protects the confidentiality of the information. This includes clear communication to all internal/external stakeholders once approved by the Chief Technology Officer.
- All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of security incidents, or vulnerabilities that might have an impact on the security of Infocentric information assets.
- Information security incidents and vulnerabilities will be reported as soon as practical to the Chief Technology Officer.
- Where a security incident has the potential to affect a Customer there will be formal communications to inform the Customer within 8 hours of incident detection.
- Record and respond to security incidents to prevent further damage, restore business services, and recover to business-as-usual and prevent recurring incidents.
- Post-incident reviews will be conducted to identify lessons learnt and ensure
- alignment against industry best practice and developments.
- Security incident response will be tested on an annual basis to ensure response timelines are achieved.
- Security incidents will be classified and prioritised according to the following severity matrix:

Incident Rating	Definition	Requirement
Critical (P1)	A serious security incident which Investigation must commence could result in compromise of the confidentiality, integrity, or availability of data, or of the integrity or availability of a number of systems.	Investigation must commence within 4 hours of notification with the aim of completion as soon as practical.
High (P2)	A security incident which could result in compromise of the confidentiality, integrity, or availability of data, or of the integrity or availability of a single system.	Commencement within 8 hours of notification with the aim of completion as soon as practical.
Medium (P3)	A security incident which could result in compromise of data or the integrity or availability of systems but is isolated to a group of user workstations and there is a mitigation available through default configuration or difficulty of exploitation.	Commencement within 1 day of notification with the aim of completion as soon as practical.
Low (P4)	A security incident which is related to a single user workstation and is unlikely to result in compromise of data or the integrity or availability of systems.	Commencement within 2 days of notification with the aim of completion as soon as practical.
Negligible (P5)	Information request or enquiry.	Commencement within 3 days of notification with the aim of completion as soon as practical.

9. Network Security – To prevent unnecessary access to information and information systems, Infocentric will:

- Protect networks and communications from unauthorised access, fraudulent insertion of data, malicious code and denial of service.
- Place assets in appropriate network segments, and control the flow of information across network boundaries.
- Filter or block inappropriate, malicious or other unauthorised content entering or leaving Infocentric.
- Secure any information exchanged within Infocentric and with external parties.

10. Security Patch Management – To prevent exploitation of known weaknesses, Infocentric will:

- Apply security patches or compensating controls according to information system and patch criticality, and with minimal operational impacts in-line with Infocentric Patch Management Standards.
- A risk assessment must be performed on all applicable exposures to determine priority of identified patches.
- Critical systems must be prioritised first for deployment of patches, these include:
  - Servers and devices that exist in the DMZ.
  - Systems storing, transmitting and/or managing any type of information considered sensitive.
- An assessment of the potential impact for deployment of patches must be completed, including consideration of any dependent systems.
- A rollback plan must be developed for high risk systems to ensure that if deployment fails or system operation cannot be resumed, that systems can be recovered to an earlier time.
- The following patch standards must be implemented to ensure timely deployment of patches:

Patch Rating	**Definition**	**Requirement**
Critical	A serious vulnerability which if exploited could result in compromise of the confidentiality, integrity, or availability of data, or of the integrity or availability of systems. The vulnerability may also allow the propagation of malware without any user action. Typically, critical vulnerabilities may have public exploit code available on the internet that may increase the likelihood of successful exploitation.	Patching activities must commence within 48 hours of notification with the aim of completion as recommended within the guidelines. If a patch is not yet available, any vendor recommended configuration changes should be implemented to reduce risk to the environment.
High	A vulnerability which if exploited could result in compromise of confidentiality, integrity, or availability of data, or of the integrity or availability of systems.	Commencement within 30 days of notification with the aim of completion as recommended within the guidelines.
Medium	A vulnerability which if exploited could result in compromise of data or the integrity or availability of systems but there is a mitigation available through default configuration or difficulty of exploitation.	Commencement within 60 days of notification with the aim of completion as recommended within the guidelines.
Low	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.	Commencement within 365 days of notification with the aim of completion as

		recommended within the guidelines.

11. Policy & Standards Management – To prevent and deter insecure behaviour, Infocentric will:

- Publish, communicate and maintain this policy for meeting Infocentric and

12. Systems & Process Development – To prevent change to, or acquisition of, information systems from introducing vulnerabilities, Infocentric will:

Include information security controls into the design, creation and modification of information systems.

- Control the migration of information system changes into production.
- Protect source code and test data during development and testing.
- Secure desktop applications developed or configured by end users.

13. Supplier Management – To prevent loss of information security where external parties are handling Infocentric information, Infocentric will:

- Manage risks arising from external parties handling Infocentric information.
- Not allow supplier access to Infocentric production information until supplier
- security is assessed by the Chief Executive Officer as having adequately effective controls.
- Identify and include appropriate information security requirements into supplier contracts, or, where terms and conditions of the contract can't be negotiated, assess publicly available information to determine if the service is within Infocentric risk appetite.
- Monitor the implementation and maintenance of required controls at the supplier site.

14. System Vulnerability Identification – To prevent exploitation of information security vulnerabilities, Infocentric will:

- Scan and test information systems to check that security controls have been securely, effectively designed and are effective in operation, and report
- vulnerabilities for remediation.
- Perform manual code reviews to align with secure coding practices.
- Biennially perform penetration tests performed by an independent third party
- provider.
- Ensure anti-malware and anti-virus mechanisms are deployed on all systems
- commonly affected by malicious software.
- Ensure that anti-malware and anti-virus mechanisms are kept current with
- malware and virus signature libraries and are configured to perform periodic
- scanning.

- Ensure that anti-malware and anti-virus mechanisms deployed cannot be altered or disabled by end-users.
- Review public-facing web applications via penetration testing or vulnerability
- assessments on an annual basis.
- Subscribe to reputable outside sources to identify security vulnerabilities and risk
- rate newly discovered security vulnerabilities.
- Remediate or mitigate critical or high vulnerabilities as soon as practical.
- Ensure that internal and external network vulnerability scans are performed after
- any significant change in the network topology.

15. Business verification of production systems – To prevent impacts to production information systems caused by business verification testing, Infocentric will:

- Manage any test data and testing activities in production environments so that appropriate information security controls can be applied.

16. Physical Security – To protect the physical security of information processing data centre or computer room protected by adequate controls, including ○ Physical perimeter controls must be applied according to risk (e.g.
facilitates, Infocentric will:

- Ensure critical or sensitive information processing facilities must be located in a perimeter fencing / gates)
    - Physical access must be limited to authorised personnel
    - Physical access must be managed
    - Controls to manage and record visitor/contractor access must be in place
    - Video monitoring must be used to deter and detect incidents and recordings are retained for a period of 12 months, where possible
    - Environmental controls and monitoring mechanisms are applied (such as adequate air-conditioning, humidity / water detection devices, fire suppression systems)
    - Adequate provision of power supply and UPS systems.

- Public access, delivery and loading areas must be segregated from information processing facilities.

17. Disaster Recovery – To ensure continued operation in the event of a business continuity event, Infocentric will:

- Develop back and recovery procedures for information systems.
- Educate Infocentric employees on their accountabilities, roles and responsibilities.
- Annually train Infocentric employees on their area of responsibility.
- Define Service Level Agreements to ensure recovery of systems is aligned with business criticality.
- Annually test backup and recovery procedures to ensure business impact is reduced in the event of a business disruption.

- Ensure that any on-site or off-site backup are encrypted.

B. INFORMATION SECURITY MANAGEMENT AND GOVERNANCE FRAMEWORK

Background

This information security management framework outlines how Infocentric manages implementation of the information security controls framework (above), govern information security, and provide assurance to internal and external parties (audit and regulators) that our information is protected.

Policy statements

18. Information Security Management – Infocentric will:

- Implement and maintain appropriate information security controls within systems and processes, including those relating to supplier relationships.
- Identify changes in threats, technologies and regulatory obligations and recommend strategic actions.
- Implement a management process, to identify the information security exposures and assess information security control effectiveness in business processes, information systems, projects, sites and third-parties handling Infocentric information.
- Assess and record the potential impact on information and information systems arising from exploitation of ineffective information security controls and implement appropriate treatment plans that minimise exposures, where required.
- Allocate resources and maintain accountabilities for information security throughout all levels of the business.
- Maintain records of information security decisions and actions.

19. Information Security Assurance – Infocentric will provide assurance to the Board (as above) by:

- Monitoring the implementation of this policy to ensure the information security controls and the exposure and risk management processes are effective and sustainable, by having: Teams conduct self-assurance on the appropriate operation of information security management processes, and the implementation and effectiveness of controls.

ROLES AND RESPONSIBILITIES

Infocentric employees and contractors have responsibilities for information security, and may have additional responsibilities based on their role.

POLICY BREACHES

Any breach of this policy is also a breach of the employment terms and conditions of Infocentric, and may be subject to disciplinary action that could, for serious breaches, include termination of employment.

Any actual or suspected breaches of this policy must be reported immediately to HR. Any breach of this policy must be escalated to the Policy Owner.

POLICY EXEMPTIONS

Although compliance with this policy is mandatory, exemptions may be permitted under extraordinary circumstances where full compliance is not possible. Requests for exemptions must be endorsed by the CEO.

LEGAL OBLIGATIONS

If, in performing duties under this policy, you complied with a legal obligation that was inconsistent with this policy, you must report this inconsistency to HR.

WHERE TO GET HELP

Information Security Policy enquiries: Email *info@infocentric.com.au*