Information Security Management System Policy
Public Version

Policy Number: CS0032		Version	3
Issued by: Corporate Services		Issue Date	November 2020

1. PURPOSE

1.1 CHESS Connect is committed to implementing an Information Security Management System to ensure that information systems are appropriately protected from loss of confidentiality, integrity and availability, and ensuring against unauthorised external alteration or destruction.

1.2 Our commitment is to implement and maintain an effective and auditable Information Security Management System, setting a baseline for information security and continuing to improve the Management System.

2. SCOPE

2.1 This policy applies to all employees and affiliates of CHESS Connect, including full-time, part-time, casual employees and third-party suppliers.

2.2 This policy will commence from the issue date recorded above.

3. POLICY STATEMENT

3.1 CHESS Connect is committed to the secure management of information systems and the secure management of information systems utilising a policy framework based on the international standard for security management systems – ISO 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

3.2 CHESS Connect is to ensure that all Staff understand the importance of information security and comply with all policy, procedures and standards regarding information and information assets, and the access of any third party without assessing any potential or unauthorised access and or risk.

3.3 CHESS Connect are committed to continuously improving Information Security Management as new risks evolve.

4. WORKPLACE and THIRD-PARTY SECURITY

4.1 The Executive Management team and the Senior Management team must provide direction and support for ISMS in accordance with business requirements and relevant laws and regulations.

4.2 CHESS Connect Management, Staff and external contractors will align their risk assessment practices relating to the ISMS with the CHESS Connect Risk Management Framework. Implementing controls for identified risks, threats and vulnerabilities (Risk Management Policy)

4.3 CHESS Connect information and information systems will be exposed to risks by allowing access from external party organisations with unknown information security management systems. Where there is a business need to provide external parties access to CHESS Connect ICT systems or for them to hold CHESS Connect data, a risk assessment is carried out to identify requirements for specific information security measures. (Information Security for Supplier Relationships Policy)

4.4 CHESS Connect is responsible for performing risk assessments and evaluating third-party security control environment. A third-party supplier risk register must exist which shows the services provided along with the risk level of each third party (eg. High/Medium/Low) based on the risk assessment.

4.5 The security of digital information and ICT accessed, process, communicated to, or managed by external parties must be controlled and monitored for identified risks or threats.

4.6 All outsourcing contracts must include an agreement on acceptable security controls and a requirement that the outsourcer provide all accreditation documentation to CHESS Connect.

4.7 All CHESS Connect third party suppliers must agree to notify CHESS Connect of a cyber incident or breach that relates to any data, systems infrastructure or processes used in their arrangements with CHESS Connect. All notifications of data breaches from Third Party suppliers should be sent to technology@chessconnect.org.au. (Data Breach Policy)

5. MAINTAINING COMPLIANCE

5.1 All staff of CHESS Connect must comply with this policy. A breach of this policy may lead to disciplinary action including, but not limited to, termination of employment or services.

5.2 If you become aware of this policy, immediately report it to your direct manager. If you are not comfortable reporting the breach to your direct manager, please refer your report directly to corporateservices@chessconnect.org.au

5.3 Enquiries about this policy should be directed to corporateservices@chessconnect.org.au

6. ISMS MAPPING WITH INDUSTRY STANDARD

This is included in this policy to align with the below controls from ISO27001:2013 Security Standard.

ISO27001:2013
Clause 4.4 Management System Processes.

7. OTHER RELATED DOCUMENTS

- Data Breach Policy
- Risk Management Policy
- Information Security for Supplier Relationships Policy

8. VARIATIONS & VERSION HISTORY

CHESS Connect reserves the right to vary, replace or terminate this policy and procedure from time to time.

Version	**Date Issued**	**Notes**	**By**

3	17/11/2020	Reviewed	ISMS Committee
2	29/9/2020	CEO approved for use	CEO
1	7/9/2020	Policy has been created.	Quality Standards Project Lead

Printing this document may make it obsolete. For the latest version of this policy always check the Policy and Procedures Directory