Information Security Policy

Intent

As a publicly funded supercomputing service provider and custodian of multiple data sets, Pawsey recognises the need to implement an information security policy that aligns with all statutory requirements, responds to emerging and persistent threats to our information and systems, and assures our partners that we are managing our environment and processes appropriately.

In regards to all of our services and datasets, Pawsey seeks to deliver the following core principles of information security:

1. **Confidentiality** – to prevent unauthorised disclosure of information.
2. **Integrity** – to assure the consistency, accuracy and trustworthiness of information throughout its entire lifecycle (in transit and at rest).
3. **Availability** – provide reliable access to information by authorised entities when needed.

Scope

Pawsey adopts the Australian Government's *Protective Security Policy Framework* (PSPF) as the foundation of its security policy processes, with CSIRO the primary security liaison partner in their role as the Pawsey Centre Agent.

This policy and associated standards, guidelines and procedures apply to:

1. All staff, users, visitors, contractors, and other third parties who in the course of their activities have access to Pawsey information or information resources.
2. Pawsey managed and administered information resources such as infrastructure, services and information systems.
3. Physical and electronic copies of Pawsey information collected, stored or transmitted via any method.

Statements

1. The Pawsey Executive Director is ultimately responsible for the governance, implementation, and oversight of Pawsey's protective security practices.
2. Pawsey will maintain a strong protective security culture evidenced through regular security awareness programs, effective system configurations (including change management), audits, formal reporting, and accessible security training.
3. As part of its broader risk management practices, Pawsey adopts a consistent and balanced risk-based approach to secure its information against threats. Major information security risks will be included in Pawsey's strategic risk management reporting.

4. All individuals who use or have access to Pawsey information or system resources must adhere to this policy at all times.
5. All users handling information at Pawsey must do so in an appropriately secure manner, including but not limited to:
    - Complying with all security standards and procedures and observing the security guidelines;
    - Complying with all applicable legal, statutory, contractual or regulatory requirements including the Australian Privacy Principles; and
    - Promptly reporting encountered or suspected security incidents or acts of misuse as defined in policy or prescribed in procedures.
6. Pawsey information assets must be individually identified, classified and protected throughout the entire asset lifecycle using appropriate security controls as outlined by the PSPF.
7. Access to information and information resources must be granted in accordance with the business need and on the basis of the "need to share" principle.
8. A suite of standards, guidelines and procedures supporting this policy will be maintained by Pawsey, and will be regularly reviewed and refined to reflect changes in business needs or the wider threat environment.
9. Temporary exemptions from Pawsey security standards and procedures must be sought from the Executive Director (or authorised delegate) prior to undertaking any alternative handling process. Formal approval in the form of a digitally signed email or signed letter must be obtained prior to implementation of any alternatives.

Roles and Responsibilities

Note: Multiple roles below may be filled by a single FTE.	
Executive Director	Endorses and is ultimately accountable for information security. Provides support for the development, implementation and maintenance of this policy and associated standards, guidelines and procedures. The role also considers and, where appropriate, grants temporary exemptions from security standards and procedures.
Chief Information Security Officer (CISO)	The CISO provides strategic direction for the implementation of this Policy, standards, guidelines and procedures, and oversees the operational management of information security personnel.
IT Security Adviser (ITSA)	The ITSA coordinates information security activities and is the first point of contact on operational information security matters. The ITSA may be assisted by Information Technology Security Officers (ITSOs) who provide operational support.
IT Security Officer (ITSO)	ITSOs may be nominated by the ITSA or CISO as distributed first points of contact on information security matters for assigned information resources.

Agency Security Advisor (ASA)	The ASA is responsible for the day-to-day performance of protective security functions.
All users handling information at Pawsey	All individuals who use or have access to Pawsey information or information resources are responsible for policy adherence at all times.

Definitions

Information Asset	Any information that has value to Pawsey or the Commonwealth.
Information Resource	Any item that is used to store, process or transmit information assets.

Approvals

Document Code	INFOSEC001
Version	1.0
Policy Owner	Executive Director
Approved By	Executive Director
Approved On	4 May 2016
Revised On	-
Next Revision	4 May 2019
Enquiries	IT Security Adviser (ITSA) – ITSA@pawsey.org.au