ICT Document No. WhoG-130
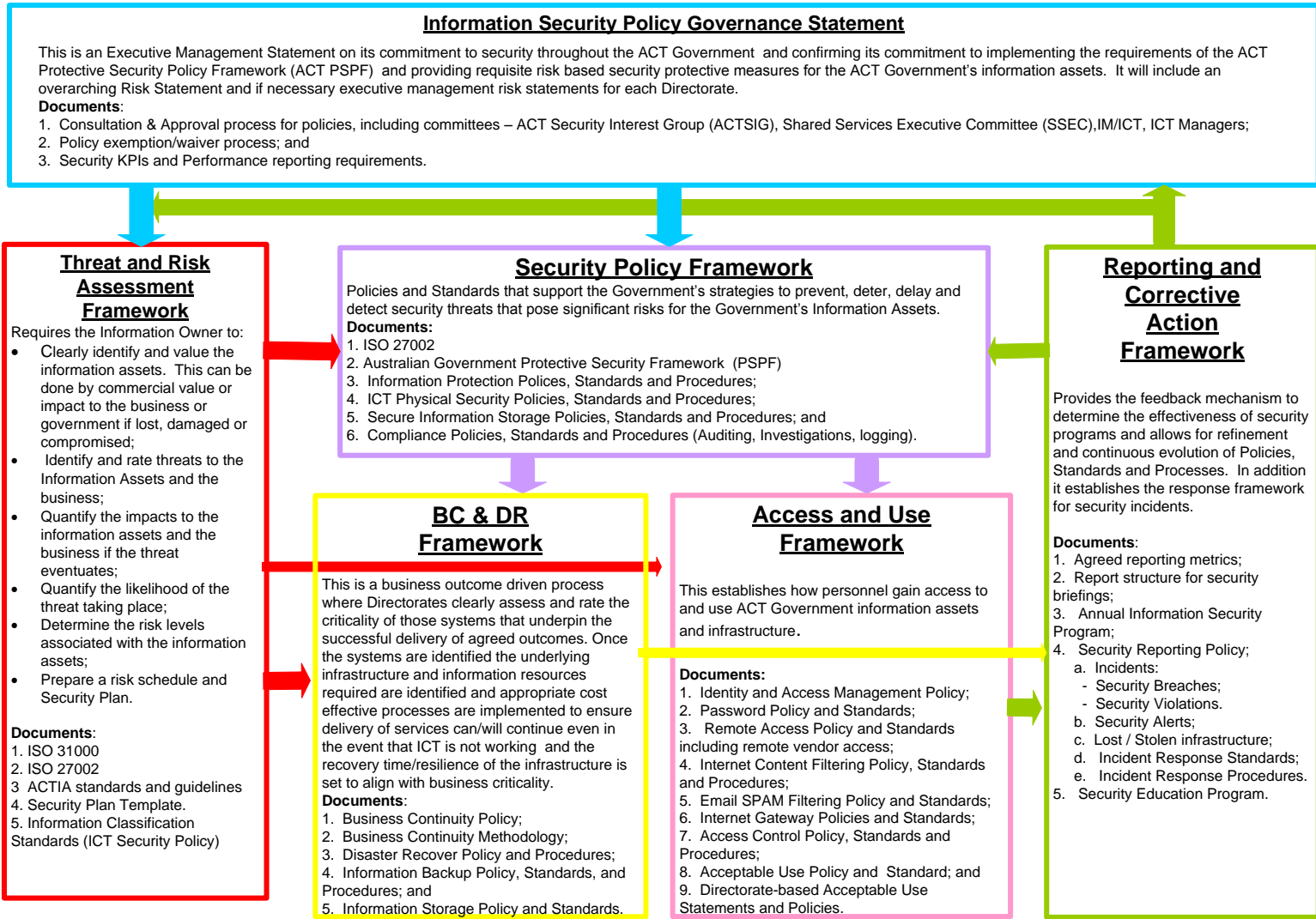
Information Security Policy Framework

Version 1.6

Updated June 2017

Approved by Executive Director,

Shared Services ICT

Error! Unknown document property name. Shared Services ICT Information Securit

Framework

Information Security Policy Governance Statement

This is an Executive Management Statement on its commitment to security throughout the ACT Government and confirming its commitment to implementing the requirements of the ACT Protective Security Policy Framework (ACT PSPF) and providing requisite risk based security protective measures for the ACT Government's information assets. It will include an overarching Risk Statement and if necessary executive management risk statements for each Directorate.

Documents:
1. Consultation & Approval process for policies, including committees – ACT Security Interest Group (ACTSIG), Shared Services Executive Committee (SSEC),IM/ICT, ICT Managers;
2. Policy exemption/waiver process; and
3. Security KPIs and Performance reporting requirements.

Threat and Risk Assessment Framework

Requires the Information Owner to:
- Clearly identify and value the information assets. This can be done by commercial value or impact to the business or government if lost, damaged or compromised;
- Identify and rate threats to the Information Assets and the business;
- Quantify the impacts to the information assets and the business if the threat eventuates;
- Quantify the likelihood of the threat taking place;
- Determine the risk levels associated with the information assets;
- Prepare a risk schedule and Security Plan.

Documents:
1. ISO 31000
2. ISO 27002
3 ACTIA standards and guidelines
4. Security Plan Template.
5. Information Classification Standards (ICT Security Policy)

Security Policy Framework

Policies and Standards that support the Government's strategies to prevent, deter, delay and detect security threats that pose significant risks for the Government's Information Assets.

Documents:
1. ISO 27002
2. Australian Government Protective Security Framework (PSPF)
3. Information Protection Polices, Standards and Procedures;
4. ICT Physical Security Policies, Standards and Procedures;
5. Secure Information Storage Policies, Standards and Procedures; and
6. Compliance Policies, Standards and Procedures (Auditing, Investigations, logging).

Reporting and Corrective Action Framework

Provides the feedback mechanism to determine the effectiveness of security programs and allows for refinement and continuous evolution of Policies, Standards and Processes. In addition it establishes the response framework for security incidents.

Documents:
1. Agreed reporting metrics;
2. Report structure for security briefings;
3.   Annual Information Security Program;
4.   Security Reporting Policy:
   a. Incidents:
     - Security Breaches;
     - Security Violations.
   b. Security Alerts;
   c. Lost / Stolen infrastructure;
   d.   Incident Response Standards;
   e.   Incident Response Procedures.
5.   Security Education Program.

BC & DR Framework

This is a business outcome driven process where Directorates clearly assess and rate the criticality of those systems that underpin the successful delivery of agreed outcomes. Once the systems are identified the underlying infrastructure and information resources required are identified and appropriate cost effective processes are implemented to ensure delivery of services can/will continue even in the event that ICT is not working and the recovery time/resilience of the infrastructure is set to align with business criticality.

Documents:
1. Business Continuity Policy;
2. Business Continuity Methodology;
3. Disaster Recover Policy and Procedures;
4. Information Backup Policy, Standards, and Procedures; and
5. Information Storage Policy and Standards.

Access and Use Framework

This establishes how personnel gain access to and use ACT Government information assets and infrastructure.

Documents:
1. Identity and Access Management Policy;
2. Password Policy and Standards;
3.   Remote Access Policy and Standards including remote vendor access;
4. Internet Content Filtering Policy, Standards and Procedures;
5. Email SPAM Filtering Policy and Standards;
6. Internet Gateway Policies and Standards;
7. Access Control Policy, Standards and Procedures;
8. Acceptable Use Policy and Standard; and
9. Directorate-based Acceptable Use Statements and Policies.

Error! Unknown document property name.

Appendix A

Metadata

Owner:	Senior Manager, ICT Security
Document location:	KB0001014
Review cycle:	This policy should be reviewed every 24 months or when conditions significantly change, whichever is the shorter duration.

Note: This is a CONTROLLED document. Any documents appearing in paper form are not controlled and should be checked against the intranet version prior to use.

Amendment history

Ver no.	Issue date	Amendment details	Author	Approval
1.0	31/10/2007	Initial release.	Peter Major – Manager, Security	Approved by Shared Services Centre Governing Committee 17 April 2007
1.1	15/01/2009	Updated 1st page footer	Annette Lock	N/A
1.5	29/05/2013	SPF box: add docs 1 and 2 TRA box: delete all docs except template, and refer to ACTIA. Cosmetic changes	HMG	N/A
	27/06/2013	First review Policy Office. Corrected the title, some typos and minor formatting.	Steven Dodt	Executive Director, Shared Services ICT
	1/10/2014	Add Bolden James classifier to Header & Footer. Cosmetic changes	Peter Major, Greg Tankard	Executive Director Shared Services ICT – Executive responsible for ICT Security
1.6	06/06/2015	Header, footer, review	Simon Bolton	Executive Director Shared Services ICT – Executive responsible for ICT Security