13.1. System Decommissioning

Objective

13.1.1. To ensure systems are safely decommissioned and that software, system logic and data are properly transitioned to new systems or archived in accordance with agency, legal and statutory requirements.

Context

Scope

13.1.2. This section discusses the retirement and safe decommissioning of systems. Specific requirements on media handling, usage, sanitisation, destruction and disposal are discussed later in this chapter. System decommissioning is the retirement or termination of a system and its operations. System decommissioning does NOT deal with the theft or loss of equipment.

Definitions

13.1.3. A system decommissioning will have one or more of the following characteristics:

- Ending a capability completely i.e. no migration, redevelopment or new version of a capability occurs;
- Combining parts of existing capabilities services into a new, different system;
- As part of wider redesign, where a capability is no longer provided and is decommissioned or merged with other capabilities or systems.

13.1.4. ICT requirements evolve as business needs change and technology advances. In some cases this will lead to the retirement and decommissioning of obsolete systems or systems surplus to requirements.

13.1.5. Security requires a structured approach to decommissioning in order to cease information system operations in a planned, orderly and secure manner. It is also important that the approach for decommissioning systems is consistent and coordinated. Sanitisation is important to eliminate any remnant data that could be retrieved by unauthorised parties. These procedures include the following:

- A migration plan;
- A decommissioning plan;
- Archiving;
- Safe disposal of equipment and media;
- Robust procedures to manage any residual data and associated risk; and
- Audit and final signoff.

13.1.6. As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data or equipment have been overlooked.

References

13.1.7.

Reference	Title	Publisher	Source
	Risk Management And Accreditation Of Information Systems Also Released As HMG Infosec Standard No. 2, August 2005	UK Centre for the Protection of National Infrastructure (CPNI)	http://www.cpni.gov.uk/Documents/Publications/2005/2005003-Risk_management.pdf
SP 800-88	**NIST Special Publication 800-88 Guidelines for Media Sanitization, Rev.1, December, 2014**	National Institute of Standards and Technology (NIST), U.S. Department of Commerce	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [PDF, 532 KB]
	Better Practice Checklist – Decommissioning Government Websites, March 2011	Australian Government Information Management Office (AGIMO)	http://agict.gov.au/policy-guides-procurement/better-practice-checklists-guidance/bpc-decommissioning

PSR references

13.1.8. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Agency Policy

13.1.9.R.01. **Rationale**

Information systems are often supported by service and supply contracts and may also be subject to obligations to provide a service, capability or information. Decommissioning of a system will require the termination of these contracts and service obligations. Other aspects of system decommission may be subject to security, regulatory or legislative requirements. An Agency policy will provide a comprehensive approach to system decommissioning from the inception of a system, thus facilitating the termination of supply contracts and service obligations while managing any risks to the Agency.

13.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3829]

When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.

Migration plan

13.1.10.R.01. **Rationale**

Once the decision to decommission a system has been taken, it is important to migrate processes, data, users and licences to replacement systems or to cease activities in an orderly fashion. It is also important to carefully plan the decommissioning process in order to avoid disruption to other systems, ensure business continuity, ensure security, protect privacy and meet any archive and other regulatory and legislative requirements. The basis of a decommissioning plan is a risk assessment.

13.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3832]

Agencies SHOULD undertake a risk assessment with consideration given to proportionality in respect of:

- scale and impact of the processes;
- data;
- users;
- licences;
- usage agreements; and
- service to be migrated or decommissioned.

13.1.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3833]

The risk assessment SHOULD include the following elements:

- Evaluation of the applications inventory and identification of any redundancies;
- Identification of data owners and key stakeholders;
- Identification of types of information (Active or Inactive) processed and stored;
- Identification of software and other (including non-transferable) licences;
- Identification of access rights to be transferred or cancelled;
- Identification of any emanation control equipment or security enhancements;
- Consideration of short and long term reporting requirements;
- Assessment of equipment and hardware for redeployment or disposal;
- Identification of any cloud-based data and services; and
- User re-training.

13.1.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3834]

Agencies SHOULD consider the need for a Privacy Impact Assessment.

13.1.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3835]

Agencies SHOULD identify relevant service and legal agreements and arrange for their termination.

Decommissioning plan

13.1.11.R.01. **Rationale**

The decommissioning of a system can be a complex process. A decommissioning plan is an important tool in properly managing the safe decommissioning of a system and in providing reasonable assurance that due process and agency policy has been followed.

13.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3838]

The decommissioning plan will be based on the migration plan and SHOULD incorporate the following elements:

- An impact analysis;
- Issue of notification to service providers, users and customers;
- Issue of notification of decommissioning to all relevant interfaces and interconnections;
- Timeframe, plan and schedule;
- Data integrity and validation checks before archiving;
- Transfer or redeployment of equipment and other assets;
- Transfer or cancellation of licences;
- Removal of redundant equipment and software;
- Removal of redundant cables and termination equipment;
- Removal of any emanation control equipment or security enhancements;
- Return or safe disposal of any emanation control equipment or security enhancements;
- Updates to systems configurations (switches, firewalls etc.);
- Equipment and media sanitisation including any cloud-based data & services(discussed later in this chapter);
- Equipment and media disposal (discussed later in this chapter);
- Any legal considerations for supply or service contract terminations;
- Asset register updates; and
- Retraining for, or redeployment of, support staff.

Archiving

13.1.12.R.01. **Rationale**

Availability and integrity requirements in respect of information may persist for legal and other statutory or compliance reasons and require transfer to other ownership or custodianship for archive purposes. This will also require assurance that the data can continue to be accessed when required (availability) and assurance that it remains unchanged (integrity).

13.1.12.R.02. **Rationale**

Confidentiality requirements must also be considered. If an information system has been processing sensitive information or contains sensitive security components, which attract special handling requirements, it will require robust purging and overwrites or destruction. There are a number of methods and proprietary products available for such purposes.

13.1.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3842]

Agencies SHOULD identify data retention policies, regulation and legislation.

13.1.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3844]

Agencies SHOULD ensure adequate system documentation is archived.

13.1.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3845]

Agencies SHOULD archive essential software, system logic, system documentation and other system data to allow information to be recovered from archive.

Audit and Final signoff

13.1.13.R.01. **Rationale**

Update the organisation's tracking and management systems to identify the specific information system components that are being removed from the inventory. To comply with governance, asset management and audit requirements, the Agency's Accreditation Authority will certify that appropriate processes have been followed. This demonstrates good governance and avoids privacy breaches.

13.1.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3850]

The Agency's Accreditation Authority SHOULD confirm IA compliance on decommissioning and disposal.

13.1.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3852]

The Agency's Accreditation Authority SHOULD confirm secure equipment and media disposal.

13.1.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3853]

The Agency's Accreditation Authority SHOULD confirm asset register updates.

13.1.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3855]

Once all security relevant activities associated with decommissioning and disposal have been completed and verified, a Security Decommissioning Compliance Certificate SHOULD be issued by the Agency's Accreditation Authority.

Final Review

13.1.14.R.01. **Rationale**

As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data, equipment, contractual or legislative, obligations have been overlooked.

13.1.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3862]

Agencies SHOULD undertake a post-decommissioning review.