| DSS05 Manage Security Services | Area: Management<br>Domain: Deliver, Service and Support |
|---|---|
| **Process Description**<br>Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring. | |
| **Process Purpose Statement**<br>Minimise the business impact of operational information security vulnerabilities and incidents. | |
| **The process supports the achievement of a set of primary IT-related goals:** | |
| **IT-related Goal** | **Related Metrics** |
| 02 IT compliance and support for business compliance with external laws and regulations | • Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss<br>• Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment<br>• Number of non-compliance issues relating to contractual agreements with IT service providers<br>• Coverage of compliance assessments |
| 04 Managed IT-related business risk | • Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment<br>• Number of significant IT-related incidents that were not identified in risk assessment<br>• Percent of enterprise risk assessments including IT-related risk<br>• Frequency of update of risk profile |
| 10 Security of information, processing infrastructure and applications | • Number of security incidents causing financial loss, business disruption or public embarrassment<br>• Number of IT services with outstanding security requirements<br>• Time to grant, change and remove access privileges, compared to agreed-on service levels<br>• Frequency of security assessment against latest standards and guidelines |
| **Process Goals and Metrics** | |
| **Process Goal** | **Related Metrics** |
| 1. Networks and communications security meet business needs. | • Number of vulnerabilities discovered<br>• Number of firewall breaches |
| 2. Information processed on, stored on and transmitted by endpoint devices is protected. | • Percent of individuals receiving awareness training relating to use of endpoint devices<br>• Number of incidents involving endpoint devices<br>• Number of unauthorised devices detected on the network or in the end-user environment |
| 3. All users are uniquely identifiable and have access rights in accordance with their business role. | • Average time between change and update of accounts<br>• Number of accounts (vs. number of authorised users/staff) |
| 4. Physical measures have been implemented to protect information from unauthorised access, damage and interference when being processed, stored or transmitted. | • Percent of periodic tests of environmental security devices<br>• Average rating for physical security assessments<br>• Number of physical security-related incidents |
| 5. Electronic information is properly secured when stored, transmitted or destroyed. | • Number of incidents relating to unauthorised access to information |

**DSS05 RACI Chart**

| Key Management Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **DSS05.01**<br>Protect against malware. | | | | | | R | I | | | | C | A | | | R | C | C | C | I | R | R | | I | R | | |
| **DSS05.02**<br>Manage network and connectivity security. | | | | | | I | | | | | C | A | | | | C | C | C | I | R | R | | I | R | | |
| **DSS05.03**<br>Manage endpoint security. | | | | | | I | | | | | C | A | | | | C | C | C | I | R | R | | I | R | | |
| **DSS05.04**<br>Manage user identity and logical access. | | | | | | R | | | | | C | A | | | I | C | C | C | I | C | R | | I | R | | C |
| **DSS05.05**<br>Manage physical access to IT assets. | | | | | | I | | | | | C | A | | | | C | C | C | I | C | R | | I | R | I | |
| **DSS05.06**<br>Manage sensitive documents and output devices. | | | | | | | | | | | I | | | | | C | C | A | | | R | | | | | |
| **DSS05.07**<br>Monitor the infrastructure for security-related events. | | | | I | | C | | | | | I | A | | | | C | C | C | I | C | R | | I | R | I | I |

**DSS05 Process Practices, Inputs/Outputs and Activities**

| Management Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | **From** | **Description** | **Description** | **To** |
| **DSS05.01 Protect against malware.**<br>Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam). | | | Malicious software prevention policy | APO01.04 |
| | | | Evaluations of potential threats | APO12.02<br>APO12.03 |

**Activities**

1. Communicate malicious software awareness  and enforce prevention procedures and responsibilities.

2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).

3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management.

4. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).

5. Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).

6. Conduct periodic training about malware in email and Internet usage. Train users to not install shared or unapproved software.

**DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)***

| Management Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **DSS05.02 Manage network and connectivity security.**<br>Use security measures and related management procedures to protect information over all methods of connectivity. | APO01.06 | Data classification guidelines | Connectivity security policy | APO01.04 |
| | APO09.03 | SLAs | Results of penetration tests | MEA02.08 |

| Activities |
|---|
| 1. Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity. |
| 2. Allow only authorised devices to have access to corporate information and the enterprise network. Configure these devices to force password entry. |
| 3. Implement network filtering mechanisms, such as firewalls and intrusion detection software, with appropriate policies to control inbound and outbound traffic. |
| 4. Encrypt information in transit according to its classification. |
| 5. Apply approved security protocols to network connectivity. |
| 6. Configure network equipment in a secure manner. |
| 7. Establish trusted mechanisms to support the secure transmission and receipt of information. |
| 8. Carry out periodic penetration testing to determine adequacy of network protection. |
| 9. Carry out periodic testing of system security to determine adequacy of system protection. |

| Management Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **DSS05.03 Manage endpoint security.**<br>Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements of the information processed, stored or transmitted. | APO03.02 | Information architecture model | Security policies for endpoint devices | APO01.04 |
| | APO09.03 | • OLAs<br>• SLAs | | |
| | BAI09.01 | Results of physical inventory checks | | |
| | DSS06.06 | Reports of violations | | |

| Activities |
|---|
| 1. Configure operating systems in a secure manner. |
| 2. Implement device lockdown mechanisms. |
| 3. Encrypt information in storage according to its classification. |
| 4. Manage remote access and control. |
| 5. Manage network configuration in a secure manner. |
| 6. Implement network traffic filtering on endpoint devices. |
| 7. Protect system integrity. |
| 8. Provide physical protection of endpoint devices. |
| 9. Dispose of endpoint devices securely. |

**DSS05 Process Practices, Inputs/Outputs and Activities *(cont.)***

| Management Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **DSS05.04 Manage user identity and logical access.** Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes. | APO01.02 | Definition of IT-related roles and responsibilities | Approved user access rights | Internal |
| | APO03.02 | Information architecture model | Results of reviews of users accounts and privileges | Internal |

| Activities |
|---|
| 1. Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles. |
| 2. Uniquely identify all information processing activities by functional roles, co-ordinating with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications. |
| 3. Authenticate all access to information assets based on their security classification, co-ordinating with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered. |
| 4. Administer all changes to access rights (creation, modifications and deletions) to take effect at the appropriate time based only on approved and documented transactions authorised by designated management individuals. |
| 5. Segregate and manage privileged user accounts. |
| 6. Perform regular management review of all accounts and related privileges. |
| 7. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable. Uniquely identify all information processing activities by user. |
| 8. Maintain an audit trail of access to information classified as highly sensitive. |

| Management Practice | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | Description | To |
| **DSS05.05 Manage physical access to IT assets.** Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party. | | | Approved access requests | Internal |
| | | | Access logs | DSS06.03 |

| Activities |
|---|
| 1. Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access. |
| 2. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities. |
| 3. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site. |
| 4. Instruct all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation. |
| 5. Require visitors to be escorted at all times while on-site. If an unaccompanied, unfamiliar individual who is not wearing staff identification is identified, alert security personnel. |
| 6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. Ensure that the devices record entry and trigger an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners. |
| 7. Conduct regular physical security awareness training. |

<table>
<tr><th colspan="5">DSS05 Process Practices, Inputs/Outputs and Activities <i>(cont.)</i></th></tr>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="3"><b>DSS05.06 Manage sensitive documents and output devices.</b><br>Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="2">APO03.02</td><td rowspan="2">Information architecture model</td><td>Inventory of sensitive documents and devices</td><td>Internal</td></tr>
<tr><td>Access privileges</td><td>Internal</td></tr>
<tr><th colspan="5">Activities</th></tr>
<tr><td colspan="5">1. Establish procedures to govern the receipt, use, removal and disposal of special forms and output devices into, within and out of the enterprise.</td></tr>
<tr><td colspan="5">2. Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.</td></tr>
<tr><td colspan="5">3. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.</td></tr>
<tr><td colspan="5">4. Establish appropriate physical safeguards over special forms and sensitive devices.</td></tr>
<tr><td colspan="5">5. Destroy sensitive information and protect output devices (e.g., degaussing of electronic media, physical destruction of memory devices, making shredders or locked paper baskets available to destroy special forms and other confidential papers).</td></tr>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4"><b>DSS05.07 Monitor the infrastructure for security-related events.</b><br>Using intrusion detection tools, monitor the infrastructure for unauthorised access and ensure that any events are integrated with general event monitoring and incident management.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td>Security event logs</td><td>Internal</td></tr>
<tr><td>Security incident characteristics</td><td>Internal</td></tr>
<tr><td>Security incident tickets</td><td>DSS02.02</td></tr>
<tr><th colspan="5">Activities</th></tr>
<tr><td colspan="5">1. Log security-related events reported by infrastructure security monitoring tools, identifying the level of information to be recorded based on a consideration of risk. Retain them for an appropriate period to assist in future investigations.</td></tr>
<tr><td colspan="5">2. Define and communicate the nature and characteristics of potential security-related incidents so they can be easily recognised and their impacts understood to enable a commensurate response.</td></tr>
<tr><td colspan="5">3. Regularly review the event logs for potential incidents.</td></tr>
<tr><td colspan="5">4. Maintain a procedure for evidence collection in line with local forensic evidence rules and ensure that all staff are made aware of the requirements.</td></tr>
<tr><td colspan="5">5. Ensure that security incident tickets are created in a timely manner when monitoring identifies potential security incidents.</td></tr>
</table>

**DSS05 Related Guidance**

| Related Standard | Detailed Reference |
|---|---|
| ISO/IEC 27002:2011 | Code of practice for information security management |
| NIST SP800-53 Rev 1 | Recommended Security Controls for USA Federal Information Systems |