Forcepoint Cloud Services - Information Security Statement

Objectives

Forcepoint cloud services are delivered from computer systems in multiple data centres located around the globe. Forcepoint are committed to maintaining the confidentiality, integrity and availability of these computer systems and the information processed on them.

Governance

Forcepoint cloud services have an information security policy that reflects both this commitment and the legal and regulatory requirements of the locations in which we operate.

Risk assessments are conducted to identify information assets, the threats and vulnerabilities to them and the potential impact of security failures affecting those assets. Options for the treatment of risks are identified and evaluated. Security controls are selected and implemented to address identified risks. Monitoring procedures are in place to detect errors in information processing, security events and measure the effectiveness of security controls.

Forcepoint cloud services have been certified to the ISO 27001 standard since September 2006 and Cloud Security Alliance STAR since May 2015 .External audits are conducted to ensure organisational compliance with security policies, procedures and the certification standards annually.

Information security policies, standards and procedures are reviewed on an annual basis to ensure that they appropriately protect information assets.

Controls

An overview of information security objectives and the controls applied to meet them can be found overleaf.

Objective: Provide management direction and support for information security objectives.

- An information security policy has been approved and distributed to employees;
- The information security policy is reviewed regularly.

Objective: Manage information security inside the organisation.

- Management actively support information security activities within the organisation;
- Information security roles and responsibilities are clearly defined;
- Security forums and mailing lists are monitored for new threats and vulnerabilities;
- Risk assessments are undertaken on an ongoing basis;
- The efficacy of policies, procedures and controls is audited on a quarterly basis;
- Third party suppliers go through rigorous screening and selection procedures.

Objective: Identify and protect information assets.

- Information assets are identified and have a logical owner assigned;
- An inventory of information assets is maintained;
- Information assets are classified, labelled and handled as per documented procedures.

Objective: Ensure that employees are suitable for their assigned roles, aware of their information security responsibilities and leave the organisation in an orderly manner.

- The recruitment process includes competence and background verification checking;
- Employee contracts include confidentiality clauses, reference information security responsibilities and indicate penalties for non-compliance with policy;
- There is a formal disciplinary process in place;
- Employees receive information security awareness, education and training;
- There is a formal procedure for return of assets and revocation of access rights on exit.

Objective: Protect information processing areas and assets from unauthorised physical access and environmental threats.

- Production systems are housed in leading data centres with strong physical entry controls, 24x7 security staff and CCTV monitoring;
- Documented procedures are in place to ensure that physical access is limited to authorised persons;
- Documented procedures are in place to ensure that all access is logged and monitored;
- Production systems are housed in leading data centres with redundant power and cooling systems.

Objective: Ensure the correct operation of information processing systems, minimise the risk of failures and ensure that systems can be replaced in the event of failures.

- Operating procedures are documented, maintained and made available to the appropriate staff;
- Operational changes to production environments are controlled by documented procedures;
- Production and development environments are kept separate;
- System capacity is monitored, capacity requirements are projected and planned for;
- The availability, performance and correct operation of the entire system is monitored at all times;
- The availability, performance and correct operation of all system components are monitored at all times;
- Acceptance tests are defined and completed prior to the deployment of new systems and upgrades;
- Backup copies of information systems, software, configuration and data are taken and tested regularly.

Objective: Detect unauthorised information processing activities.

- Activities undertaken in the management applications are logged;
- All hosts log events to local file systems and a centralised database;
- Procedures for the regular examination of these outputs are documented;
- Event logging systems and log information are protected from unauthorised access;
- All hosts are synchronised to an accurate time source.

Objective: Control access to information, ensuring appropriate access for authorised users and preventing access for unauthorised users.

- There is a documented process for the assignment and removal of system access;
- Users are assigned only those permissions necessary for completion of their roles;
- There is a documented process for the review of system access lists;
- Users are aware of their responsibilities to secure and protect system access;
- Systems enforce good practice in the selection and use of passwords.

Objective: Prevent unauthorised access to network services, operating systems and applications.

- Access to production networks is provided by a VPN solution requiring dual factor authentication;
- VPN connections to production networks are time limited;
- Login to the VPN is required from all locations, including corporate networks;
- Each user is uniquely identified, generic user identifiers are not permitted;
- Inactive administration sessions are automatically terminated.

Objective: Maintain the security of information systems during the systems development and maintenance process.

- The design and functional specification of proposed changes to information systems are reviewed by information security staff;
- A revision control system is used to ensure that software changes are controlled and audited;
- Quality assurance processes are in place to ensure that code and software releases meet documented expectations;
- System changes are controlled, documented and approved by management prior to implementation;
- System changes include acceptance tests, escalation contacts and a rollback procedure;
- System configurations are centrally managed, monitored and audited using a configuration management system;
- System configuration files are deployed from a revision control system to ensure that system changes are controlled and audited.

Objective: Ensure that security issues are reported, fixed and that action is taken to prevent recurrence.

- Employees are required to report information security issues using a documented procedure;
- There is a documented procedure for the management of information security issues;
- Information security issues are logged, fixed and actions are taken to prevent recurrence.

Objective: Minimise the risk of interruptions to service caused by major failures of information processing systems or locations.

- There is a documented business continuity plan;
- We have multiple production clusters and in the case of a service or cluster failing load will automatically be switched to another location;
- We do not perform testing on production systems however these failover capabilities are routinely exercised during normal operational maintenance;
- In the event of a disaster affecting one of our business offices the hosted infrastructure is entirely separate from the corporate infrastructure and can be administered from alternative locations indefinitely.

Objective: Comply with contractual, legal and regulatory requirements.

- Forcepoint identify and comply with the legal requirements of the regions in which we operate;
- Employees are made aware of their responsibility to observe intellectual property and data protection legislation;
- Systems undergo technical compliance checking on a regular basis, issues raised by these tests are logged and tracked to completion.