

Addressing security in third party agreements

Policy #: 6.2.3

Version #: 1.0

Approved By: John Doe, CEO

Effective Date: March 14, 2010

Purpose: To ensure that agreements with third parties address all relevant security requirements.

Scope: This policy applies to all ORGANIZATION NAME workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, authorized third parties, and anyone else granted access to sensitive information by ORGANIZATION NAME.

Policy: ORGANIZATION NAME will ensure that all agreements with third parties involving accessing, processing, communicating or managing ORGANIZATION NAME's information or information processing facilities and/or adding products or services to information processing facilities should cover all relevant security requirements.

ORGANIZATION NAME will consider the following factors and choose those appropriate for inclusion in the third party agreement:

- 1) ORGANIZATION NAME's information security policy;
- 2) Controls to ensure asset protection potentially including;
 - a. Procedures to protect organizational assets, information, software, and hardware;
 - b. Physical protection controls and mechanisms;
 - c. Malicious software protection;
 - d. Incident identification, response, and management procedures;
 - e. Assurances that information or assets will be returned or permanently destroyed at the end of the agreement period or at a certain point in time;
 - f. Confidentiality, integrity, and availability of the assets; and
 - g. Restrictions on copying or disclosing information.
- 3) User and administrator training in methods, procedures, and security;
- 4) Ensuring user awareness for information security responsibility and issues;
- 5) Provision for the transfer of personnel if appropriate;
- 6) Software installation and maintenance responsibilities;
- 7) Clear reporting structure and agreed reporting formats;
- 8) Clear and specific change management;
- 9) Comprehensive access control policy including;
 - a. Reasons, requirements, and benefits of third party access;
 - b. Permitted access methods and unique user identification requirements;
 - c. Authorization process for user access and privileges;
 - d. Require a list of authorized users and their rights and privileges;
 - e. Statement that all access not explicitly authorized is forbidden;
 - f. Process for revoking access rights and/or terminating connectivity between systems;
- 10) arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;
- 11) a description of the product or service to be provided, and a description of the information to be made available along with its security classification;

- 12) the target level of service and unacceptable levels of service;
- 13) the definition of verifiable performance criteria, their monitoring and reporting;
- 14) the right to monitor, and revoke, any activity related to the organization's assets
- 15) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
- 16) the establishment of an escalation process for problem resolution;
- 17) service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;
- 18) the respective liabilities of the parties to the agreement;
- 19) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries;
- 20) intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;
- 21) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;
- 22) conditions for renegotiation/termination of agreements:
 - a. a contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements;
 - b. renegotiation of agreements if the security requirements of the organization change;
 - c. current documentation of asset lists, licenses, agreements or rights relating to them.

Responsibilities: Compliance and review are the responsibility of the designated Security Officer.

Compliance: Failure to comply with this or any other security policy will result in corrective actions as per the Disciplinary Process Policy. Legal actions also may be taken for violations of applicable regulations and standards such as ISO 27002, HIPAA, GLB, Sarbanes-Oxley and others.

References:

- International Standards Organization (ISO/IEC 27002, 6.2.3).

Contact:

John Doe, Security Officer
1234 Anystreet
Anywhere, IL 55555

E: John.doe@anywhere.com

P: 555.555.5555

F: 777.777.7777

Policy History: Initial effective date: March 14, 2010

Inventory of Assets

Policy #: 7.1.1

Version #: 1.0

Approved By: John Doe, CEO

Effective Date: March 14, 2010

Purpose: To achieve and maintain appropriate protection of organizational assets.

Scope: This policy applies to all ORGANIZATION NAME workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, authorized third parties, and anyone else granted access to sensitive information by ORGANIZATION NAME.

Policy: ORGANIZATION NAME will clearly identify and inventory all important assets. The asset inventory will include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.

Ownership and information classification will be documented for each of the listed assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets will be identified.

ORGANIZATION NAME will consider many different types of assets including:

- 1) Information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- 2) Software assets: application software, system software, development tools, and utilities;
- 3) Physical assets: computer equipment, communications equipment, removable media, and other equipment;
- 4) Services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- 5) People, and their qualifications, skills, and experience;
- 6) Intangibles, such as reputation and image of the organization.

Responsibilities: Compliance and review are the responsibility of the designated Security Officer.

Compliance: Failure to comply with this or any other security policy will result in corrective actions as per the Disciplinary Process Policy. Legal actions also may be taken for violations of applicable regulations and standards such as ISO 27002, HIPAA, GLB, Sarbanes-Oxley and others.

References:

- International Standards Organization (ISO/IEC 27002, 7.1.1).
- More information on how to value assets to represent their importance can be found in ISO/IEC TR 13335-3

Contact:

John Doe, Security Officer

1234 Anystreet
Anywhere, IL 55555

E: John.doe@anywhere.com
P: 555.555.5555
F: 777.777.7777

Policy History: Initial effective date: March 14, 2010

SAMPLE