|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Cloud Computing Security Policy | | | | | |
| Policy # | CPL-09-04 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457903314)

[Scope 1](#_Toc457903315)

[Policy 1](#_Toc457903316)

[Cloud Approval and Governance 1](#_Toc457903317)

[Establishing Cloud Services 2](#_Toc457903318)

[Access Controls 2](#_Toc457903319)

[Privacy Controls 2](#_Toc457903320)

[Sensitive Data Storage 2](#_Toc457903321)

[Violations 2](#_Toc457903322)

[Definitions 3](#_Toc457903323)

[References 3](#_Toc457903324)

[Related Documents 3](#_Toc457903325)

[Approval and Ownership 4](#_Toc457903326)

[Revision History 4](#_Toc457903327)

Purpose

This policy defines the specific information security requirements for establishment and use of third party (aka “cloud”) services to store or process Company X information assets without jeopardizing company data and computing resources.

Scope

This policy applies to all personnel responsible for managing Company X information assets.

This policy applies to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal email accounts are excluded.

Policy

### Cloud Approval and Governance

**Approval Required** - Use of cloud computing services for Company X business purposes must be formally authorized by the Information Technology Manager. Employees must not open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without approval

**Vendor Validation** – All third-party processing (cloud) vendors must be approved by the Information Technology Department. The Information Technology Manager must certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

**Control Compliance** – Additional control requirements adopted as part of cloud arrangements must be formally adopted into the Company X internal control framework.

### Establishing Cloud Services

**Terms of Service Approval** - For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Information Technology Manager.

**Only Preapproved Cloud Services** – Employees must only establish cloud service accounts with approved cloud service vendors that have been approved by the Information Technology Manager. [Insert list of approved vendors here. i.e. AWS, etc.]

### Access Controls

**Access Credentials** - Employees and contractors establishing login credentials at third-party (cloud) services must comply with existing Company X security requirements for secure passwords.

**Password Sharing** – Employees and contractors establishing login credentials at third-party (cloud) services must not use the same passwords as those for local accounts.

**Management Reporting** – Employees that establish login credentials at third-party (cloud) services must notify their manager and the IT department of the details of the account and the types of data being stored. An exception to this policy is made when the Information Technology Department establishes and assigns these accounts.

### Privacy Controls

**Foreign Data Transfer** – Customer personally identifiable information (PII) must not be stored in third-party (cloud) environments that are located in foreign countries.

### Sensitive Data Storage

**Data Storage Approval** – The Information Technology Manager must approve the types of data that may be stored in third-party (cloud) environments.

**Personal Data Storage** - Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Custodian** - Guardian or caretaker of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Confidential Information (Sensitive Information)** – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement.

**Cloud Services** – Cloud services are any third-party service that processes or stores data outside of the Company network. e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal email accounts are excluded.

**Owner** - The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

**Third Party (Partner) –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 9.0 – Network Security

ISO 27002: 13.1 Network security management

HIPAA: Integrity §164.312(c)(1)

NIST: SC-1 System and Communications Protection Policy and Procedures

PCI: R3. Protect stored cardholder data

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |