Cloud Security Compliance Documentation

Cloud Security Compliance Documentation

Table of Contents

Cloud Security Compliance Documentation

1. Purpose

This policy ensures the confidentiality, integrity and availability of data stored, accessed and manipulated using cloud computing services. It establishes a framework of responsibility and actions required to meet regulatory requirements and security guidelines for cloud computing.

2. Scope

This policy covers systems handling data listed in Section 2.1 below. All services within the cloud environment that fall into this category will be subject to the requirements specified within this policy. Therefore, it applies to every server, database and other IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. The requirements apply to new and existing installations. Every user who interacts with company IT services is also subject to this policy. The security control requirements are applicable for all approved cloud systems.

2.1. Information Types

This policy applies to all customer data, personal data and other company data defined as sensitive by the company's data classification policy. The sensitive data types covered by this policy include:

Identity and authentication data:

- Passwords
- Cryptographic private keys
- Hash tables

Financial data:

- Invoices
- Payroll data
- Revenue data
- Accounts receivable data

Proprietary data:

- Software test and analysis
- Research and development

Employee personal data:

- Names and addresses
- Social Security numbers
- State-issued driver’s license number
- State-issued identification card number
- Financial account numbers, including security code, access code or password admitting access to the account
- Medical and/or health insurance information

3. Ownership and Responsibilities

By defining clear ownership and responsibilities for each role, this Cloud Security Policy aims to ensure the confidentiality, integrity, and availability of Compu-Global-Hyper-Mega-Net's cloud resources and data while minimizing the potential impact of security incidents.

Chief Information Security Officer (CISO)

The CISO holds overall responsibility for ensuring the security and compliance of Compu-Global-Hyper-Mega-Net's cloud infrastructure and services. Their primary duties include:

- Establishing and maintaining the Cloud Security Policy and related guidelines.

- Collaborating with other stakeholders to define Compu-Global-Hyper-Mega-Net's risk appetite and cloud security objectives.
- Overseeing the implementation and enforcement of cloud security controls and measures.
- Conducting regular risk assessments and audits of the cloud environment and provider to identify potential vulnerabilities.
- Providing executive leadership and support for cloud security initiatives.
- Staying informed about emerging threats and trends in cloud security and adapting strategies accordingly.
- Ensuring the cloud security team and cloud administrators have the necessary resources and training to fulfill their roles effectively.

Cloud Security Administrator

- Configuring and maintaining cloud security tools and technologies.
- Monitoring the cloud environment for security incidents, breaches, and unauthorized access attempts.
- Responding to and investigating security alerts and incidents promptly.
- Managing access controls, permissions, and user identities within the cloud environment.
- Collaborating with cloud users and the cloud security team to enforce security policies and best practices.
- Implementing and monitoring multi-factor authentication (MFA) mechanisms.
- Conducting regular vulnerability assessments and coordinating the remediation of identified weaknesses.
- Assisting in the development and execution of security training and awareness programs for cloud users.

Cloud Security Team

- Conducting regular risk assessments to identify potential vulnerabilities and threats in the cloud environment.
- Developing and implementing robust security policies, standards, and procedures for cloud services.
- Monitoring and analyzing security logs, events, and incidents to detect and respond to security breaches.

- Collaborating with cloud administrators and users to address security concerns and provide guidance.
- Reviewing and approving requests for access to cloud resources, ensuring appropriate permissions and segregation of duties.
- Keeping abreast of new cloud security technologies and best practices to enhance Compu-Global-Hyper-Mega-Net's security posture.
- Performing periodic security assessments and penetration tests on cloud infrastructure and services.
- Assisting in incident response and forensic investigations in the event of a security breach.

Cloud Users

- Abiding by Compu-Global-Hyper-Mega-Net's cloud security policies, standards, and procedures.
- Using strong and unique passwords, along with multi-factor authentication where required.
- Reporting any suspicious activity or security incidents promptly to the cloud security team.
- Complying with data classification and handling guidelines to safeguard sensitive information.
- Keeping cloud applications and data up to date with the latest security patches and updates.
- Understanding and adhering to the principle of least privilege when accessing cloud resources.
- Participating in security awareness and training programs to stay informed about cloud security best practices.
- Following Compu-Global-Hyper-Mega-Net's data backup and recovery procedures to mitigate data loss risks.

4. Secure Usage of Cloud Computing Services

All cloud-based services must be approved by the CISO prior to acquisition and deployment. To ensure secure adoption and usage of cloud services, the following steps must be taken:

- Define the organization's needs and priorities.
- Define service users, both internal and external.
- Determine the type of cloud service to be adopted, including the physical and operational characteristics for SaaS, PaaS and IaaS solutions.
- Define the data types to be stored.
- Determine the security solutions and configurations required for encryption, monitoring, backups, etc.
- Generate a list of past security incidents involving this cloud provider.
- Request available security certifications.
- Obtain copies of agreements with the provider, including SLAs.

4.1 Inventory

The cloud security administrator and cloud security team must perform an inventory of cloud services in use at least quarterly. Unused services, including resources such as instances, buckets, etc,. shall be reviewed for long-term data retention needs and deletion.

4.2. Approved Services

Amazon Web Services (AWS) is the approved provider of cloud computing for Compu-Global-Hyper-Mega-Net. No other cloud services may be utilized without written approval from the CISO. AWS is approved to provide all aspects of Platform as a Service (PaaS) and Software as a Service (Saas). Department heads are authorized to scale their use of services, based on the needs of the department. They may contact the CISO, if needed, for help determining what structure will suit them best.

4.3 Unauthorized Services

Only the cloud-based solutions on the list of approved services specified in Section 4.2 of this document may be used. The installation of unauthorized software on organizationally owned or managed user end-point devices (e.g., workstations, laptops and mobile devices) and IT infrastructure network and systems components is restricted. The cloud security administrator must provide authorization for any third-party cloud service before it is placed into use. The introduction of any unauthorized cloud service will immediately generate a notification for IT security and block the service from use.

5. Risk Assessment

Data from the “Sensitive” tier of the Data Classification Policy shall be available at all times, per regulations, for discovery and audit. Cloud providers shall conform to these compliance requirements.

The Cloud Security Administrator and the IT Security team shall conduct a risk assessment at the following times:

- Upon the implementation of a new cloud service
- After major upgrades or updates to an existing cloud service
- After any changes to the configuration of a cloud service
- When following up on a security event or incident
- Quarterly for all existing cloud services

The cloud security risk assessment shall include the following:

- Audit results, both internal and external (cloud provider system security audit results)
- Threat and vulnerability analysis
- Regulatory compliance

6. Security Controls

Security controls have been developed to follow the National Institute of Standards and Technology (NIST) framework. This framework uses five “functions” which should be assessed and addressed to develop a strong cyber security environment, They are:

- Identify
- Protect
- Detect
- Respond
- Recover

6.1. Identify

In order to manage cyber risk, it is important to develop an understanding of the organizational environment, including systems, data and assets.

Systems

Compu-Global-Hyper-Mega-Net will be using the AWS computing environment with Virtual Private Cloud (VPC), EC2 Instances, and S3 buckets. Linux and Windows OS environments will be utilized.
Data

Multiple data types will be utilized and stored, as detailed in Section 2.1. There is a public subnet established for data that is available to the public. Non-public data will be contained in a private subnet and S3 buckets that are logically separated from the public subnet.

Assets

On-premises physical assets will be confined to endpoints and network servers. Most assets are cloud-based and physical security will be the responsibility of AWS.

Threats

The primary threat is malicious attackers trying to gain access to sensitive data.

Insider threats from internal personnel looking to sell sensitive data is also a point of concern.

6.2. Protect

Numerous strategic and tactical measures shall be implemented to protect the systems, data and assets identified in Section 6.1.

Authorization/Access Control

Access control methods to be used shall include:

- Auditing of attempts to log on to any device on the company network
- Windows NTFS permissions to files and folders
- Role-based access model
- Server access rights
- Firewall permissions
- Web authentication rights
- Database access rights and ACLs
- Encryption at rest and in transit
- Network segregation

Access controls apply to all networks, servers, workstations, laptops, mobile devices, cloud applications and websites, cloud storages, and services.

System Security

Logical network segregation will be utilized to separate publicly accessible system parts from those only available to organization personnel.

Only CIS-compliant (Center for Internet Security) EC2 Instances shall be utilized to minimize vulnerabilities.

Monthly, the Cloud Security Administrator shall perform an assessment of security control configurations and all failed attempts of unauthorized access.

Data Protection

Sensitive data will be encrypted in transit and at rest using GPG, IPSEC or BitLocker, as appropriate for the circumstances in accordance with the Data Encryption Policy.

Routine backups will be conducted according to a set schedule to protect against data loss.

Asset Protection

Cloud computing assets are managed and protected by the cloud service provider. The Cloud Security Administrator shall review physical security audits for the Cloud

Infrastructure Provider at least semi-annually. These audits shall include a visit to at least two data centers used for the organization's resources.

Company resources shall also be inspected at least semi-annually for physical security compliance. This inspection shall include server room security and endpoint security practices by employees.

The company shall monitor the interior temperature of the server rooms and ensure that the management receives an immediate notification if the temperature varies more than 5 degrees from the baseline.

Company-owned assets will be protected with multi-factor authentication (MFA), firewalls, role-based access control, routine software updates and adherence to the standards in the physical security manual.

General Protection Measures

The IT Security Management office shall provide initial security training to all new users of cloud services and annually for all users thereafter. All users of cloud services must pass security training to maintain permissions and access to the service. Users will sign their agreement to the Acceptable Use Policy (AUP) and Network/Cloud Security Policy.

6.3. Detect

Compu-Global-Hyper-Mega-Net shall put into place tools for centralized visibility of the cloud service infrastructure, such as VPC flow logs, ClodTrails and Cloudwatch. These tools shall offer traffic analysis, configuration monitoring and assessment, and alerts for configuration issues and unauthorized/suspicious activity that is detected.

6.4 Respond

The Cloud Security team will respond immediately to all alerts for intrusion attempts or malicious activity. Detailed response procedures are in the Incident Response SOP.

The Cloud Security Administrator shall ensure the Cloud Security Team is trained on the response procedures and regular testing is conducted.

6.5. Recover

In the event of a data breach, both the cloud provider and the cloud security administrator shall perform an assessment of the systems and report the findings as detailed in the Security Incident Plan SOP. Priorities for data recovery:

- All non-archived data classified as Sensitive is considered to have a priority of High.
- All archived data classified as Sensitive is considered to have a priority of Moderate.
- All data classified as Internal is considered to have a priority of Moderate.
- All data classified as Public is considered to have a priority of Low.

6.6. Mobile Security Requirements

Cloud security shall include mobile security controls to prevent malware infection on company mobile devices and privately owned devices used to access the organization's cloud services. Any device found without anti-malware protection shall be quarantined.

7. Enforcement

Employees who attempt to use unauthorized services or misuse resources in violation of the AUP and other applicable policies shall have their permissions revoked and be referred to HR for potential disciplinary action. If cleared to continue working by HR, they shall be required to pass security training before having their access restored.

8. References/Related Documents

The following is a list of all documents related to IT and cloud security policy and procedures:

- Acceptable Use Policy
- Data Protection and Encryption Policy

- Password Policy
- Risk Assessment Policy
- Workstation Security Policy
- Cyber and Data Security Incident Response Plan

9. Definitions

Cloud Computing:	The full ecosystem of services furnished by the cloud provider, including: hardware, storage, networking appliances, servers, software, and stored data.
Data:	Any information stored in digital format on any type of media (hard drive, server, USB, compact disk, cloud storage, etc.)
Encryption:	A method of scrambling data into code that looks like gibberish until unlocked with a password or digital key.
Endpoint/ Workstation:	The computer and monitor that an individual worker uses, either desktop or laptop.

10. Sources

- Netwrix
- National Institute of Standards and Technology

11. Revision History

07/07/2023 -- “Compliance Documentation” created by Chris Bennett