Security Practices

SysCloud ensures that your data is secure, available, and accessible at all times. We have different layers of security measures to make sure that your data is private and safe.

How we secure backup archives?

Access management: Centralized identity and access management is used. Access to Application and Infrastructure is provisioned in accordance with the principle of least privilege and access is only provided on a need-to-know basis. Role based access control (RBAC) is implemented and roles are granted to users to control access to Infrastructure and Applications. User access is reviewed on a quarterly basis to reassess validity of access granted to a user.

Multi-Factor authentication: SysCloud mandates the use of a two-factor (2-step) authentication mechanism for all access to production environments and resources. Network Security: SysCloud applications are hosted on a Virtual Private Network and access to production systems is restricted from the public internet. Network segmentation helps SysCloud prevent a threat actor from directly accessing the production systems.

Logging and monitoring: Logs are monitored and alerts and alerts are configured to identify security incidents in real time. Incidents are logged and tracked through an Incident Management Tool. Incidents are escalated as per the escalation matrix and are tracked to closure. Root cause analysis is performed to identify the corrective action and preventive action.

Vulnerability and security tests: Regular vulnerability and security tests are conducted to proactively identify and fix potential security vulnerabilities in Infrastructure and Applications. Identified vulnerabilities are rated using Common Vulnerability Scoring System (CVSS). CVSS is an open trusted framework that standardizes vulnerability reporting and provides a consistent view of vulnerability levels. Action plans are identified and vulnerabilities are tracked to closure. Retesting is performed to confirm vulnerabilities are closed.

Backups: Data is backed up on a real-time basis to ensure high-availability of data and periodic recovery operations are conducted to assess the integrity of the backup.

Patching: Security patches prevent threat actors from exploiting underlying vulnerabilities. Patches updates are checked periodically for latest updates. Patches are tested in a test environment and approved prior to deployment.

Third-party audits: SysCloud obtains SOC 2 Report from AWS on an annual basis to assess the design and operating effectiveness of controls implemented by AWS.

SysCloud application security practices

Identity and access management: SysCloud mandates the use of a unique User ID for each employee. Where passwords are employed for authentication, SysCloud's password policies are enforced including password expiration, restrictions on password reuse, and sufficient password strength. A centralized role management is used to manage Role based access control (RBAC) of users to production systems and resources.

Multi-factor authentication: SysCloud mandates use of a two-factor (2-step) authentication mechanism for all access to production environments and resources.

Vulnerability management: SysCloud security team manages the Vulnerability Management Program. Security Team scans for security threats using leading security tools, performs automated and manual penetration testing, secure application and configuration reviews. The Security Team is responsible to track and follow-up on vulnerabilities.

Upon identification of a vulnerability, Security Team logs the vulnerability, prioritizes according to the severity and assigns an owner. Security Team tracks until the vulnerability has been remediated and retested.
Safeguarding data at rest and in transit: Data is classified in terms of criticality and sensitivity. Multiple security controls are places to protect data at rest and transit including access control, tokenization and encryption. SysCloud application is accessed by users via the Internet and protected by Transport Layer Security (TLS).

Secure software development lifecycle: SysCloud has defined policies and procedures to manage Development and Maintenance activities. Security risks are evaluated for every project and corresponding mitigating controls are documented. Developers are trained on secure coding guidelines. Every project undergoes peer code review and multi-layered security testing. All changes undergo automated and manual testing to identify vulnerabilities. Source code changes are performed by developers and changes are stored in a version control system. Every change is moved to production only after successful quality testing.

Logging and monitoring: Administrative and user activities within the SysCloud production systems is logged. These logs are reviewable by the Security Team on an as-needed basis. All connections to the production environment are forced by network-level controls; these centralized auditing of connections into the production environment, and allow for control over production access

SysCloud corporate security practices

Information security policies and procedures: SysCloud has a set of defined Information Security Policies and procedures. These policies cover a broad range of security related procedures from corporate policies to policies that every employee must follow. These policies cover areas such as Access Management, incident management, Secure Software Development and Change Management, Business Continuity and Disaster Recovery etc.

Information security function and team: SysCloud has a dedicated function of information security professionals. The Team is responsible for designing the company's security policies and internal defence systems, processes for secure development and security review, and building customized security infrastructure. Some of the activities undertaken by the Internal Security Teams are:

- Review the security design and perform post implementation-level reviews, advise on security risks for a project.
- Monitors for suspicious activity on SysCloud's networks.

- Enforce compliance to defined policies through internal audits and security evaluations.
- Partners with Cyber Security Subject Matter Experts to conduct periodic endpoint security testing.
- Compliance and adherence to the Vulnerability Management Program. Supporting internal teams to remediate issues identified as part of vulnerability scans.

Personnel security: All employees working at SysCloud are required to acknowledge in writing their acceptance to SysCloud policies and procedures. Employees are mandated to execute non-disclosure agreements and reaffirm annually their understanding and compliance with SysCloud's employee's handbook.

Upon hire, SysCloud engages an independent Background verification agency to verify the education, previous employment checks and Criminal records check.

Information security training: SysCloud has a defined Information Security Awareness Training Program. All employees undergo security training as part of the onboarding process. In addition, all the employees undergo annual training and depending on the job roles and responsibilities targeted training programs are conducted. Employees are also trained to tag confidential data and procedures to be followed while handling customer data.

Access management: Upon hire, an employee is assigned a User ID by Human Resources and a limited set of privileges are granted such as email and drive access. Employees are granted additional access based on job function, roles and responsibilities. Every user access request is processed only upon receiving appropriate approval in accordance with defined policies and procedures. In addition, access rights and levels are based on the principles of least-privilege and need-to-know basis. Upon Separation, user access is revoked to SysCloud's Infrastructure and Application.

Incident management: SysCloud has a defined incident management process for security events. Incident Management procedure describes the course of action, escalation mechanism, communication protocols, mitigation and documentation.

Business continuity and disaster recovery: SysCloud has a defined Business Continuity and Disaster Recovery program to minimize service interruption due to natural disaster or other events. This program is defined with an objective to minimize the risk of a single point of failure including replication of application data in real-time to another region. SysCloud stores backups in geographically distributed regions to maintain continuity in the event of disaster in a single region.

In addition to management of backups, SysCloud has a defined business continuity plan for its operations in India. This plan is designed to enable coordinated efforts for continued operations of services to Customers.
Business Continuity plans are tested annually. Testing is performed in accordance to defined Business Continuity Plans including establishing the scope, objective and scenario. SysCloud uses various methods to perform BCP tests ranging from tabletop exercises to full-scale simulations of real-life incidents. Results of the testing are analyzed and recovery strategies are modified to achieve desired recovery timeframes. For example, during such tests, a disaster in a geographic region is simulated by taking IT systems and operational processes off-line and allowing such systems and processes to transfer to fail-over locations designated as per the Disaster Recovery Plan. During the course of the test, it is confirmed that business and operations can operate at the Disaster Recovery location. Any issues identified as part of the testing are identified and logged for remediation.

What is our process for handling security breaches or incidents?

Incident management policies: SysCloud has defined Incident Management policies and procedures. Security events that impact the confidentiality, integrity, or availability of systems or data is classified as an Incident.

As part of the Incident Response Program, the following are performed:

- Training users on security operations and incident response

- Defining playbooks and guides to ensure reliable and consistent response
- Testing is simulated taking a variety of scenarios, including insider threats and software vulnerabilities to assess the effectiveness of incident response.
- Updating Incident Management policies and procedures as necessary

Incident reporting: Incidents can be either reported by internal teams or customers by sending an email to incident@syscloud.com. On receipt of an incident, SysCloud's internal teams respond by logging and prioritizing the incident according to its severity. Events that directly impact customers are treated with the highest priority. Assigned teams complete initial triage, perform root cause analysis, identify corrective action and preventive action. An action owner and target timelines are assigned against each action plan. The status of incidents and action plans are reviewed by Management on a weekly basis.

In the event of a data breach, a team comprising of Legal, Technology and Security experts are involved and the following steps are additionally performed:

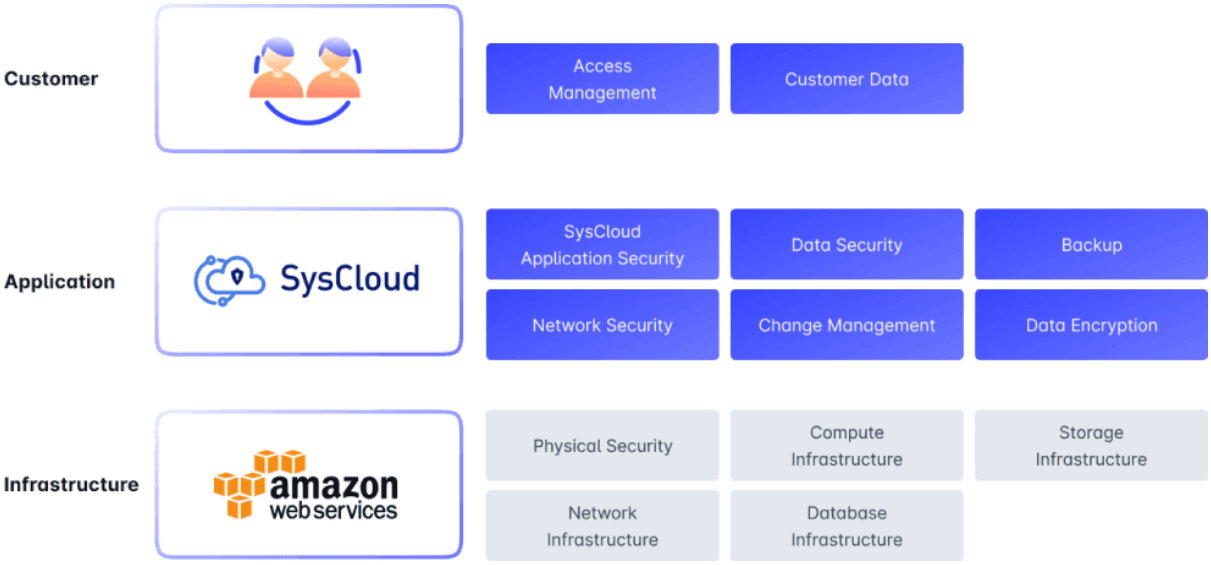
- Communication with relevant internal and external stakeholders, including notification to affected customers to meet breach or incident notification contractual obligations and to comply with relevant laws and regulations
- Gather and preserve evidence for investigative efforts

Further, post-mortem is conducted upon incident closure to determine the root cause for single events, trends spanning across multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

What are the customer's obligations for securing their backup archives on SysCloud?

Security and Compliance is a shared responsibility between SysCloud and the customer. This shared model can help the customer understand its obligations. Customers assume responsibility and management of the data and users' access within the SysCloud Application. SysCloud manages the Application, operating system (including updates and security patches) and associated Infrastructure.

As shown in the chart below, responsibilities are chalked between SysCloud and the customer:



While SysCloud is responsible for securing each aspect of the application that's under our control, customers play a key role in ensuring their teams and data are protected and secure. As the admin of a SysCloud Backup application, you have the ability to configure, use, and monitor your account in ways that meet your organization's security, privacy, and compliance needs.

This customer/SysCloud shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between SysCloud and its customers, so is the management, operation, and verification of IT controls shared.

The customer is responsible for the following:

- **User administration**: Configuring settings through the Admin Console including assigning users and modifying roles. Customize settings and choose the appropriate level of access and role for a user. Ensuring only authorized users have access to the SysCloud application.
- **Authentication**: Managing authentication to the SysCloud application and enforcing strong password security controls. Avoid sharing of user credentials.
- **Data management**: Selection of data to be backed up and also controlling the inclusions and exclusions to the data, performing cross user restore and all other functions relating to data from the admin console.

- **Backup configuration:** Configuring backup settings such as retention, categories of data to be backed up, and restrict users from deleting data.

- **Evaluate regulatory and compliance fitness**: Determining if SysCloud security practices are aligned to your compliance program. SysCloud Backup and Data protection applications are covered by SOC 1 Type 2 and SOC 1 Type 2 Attest reports. We can also provide access to additional documentation under a non-disclosure agreement to help you make an informed decision. This includes mapping of our internal practices between requirements of HIPAA, COPPA, and FERPA.

What are security certifications and what do we have?

Service Organization Controls

System and Organization Controls (SOC) Reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and related controls through a report by an independent CPA.

SOC 1 Type 2 Report provides assurance on the design and operating effectiveness of Internal Controls over Financial Reporting at Service Organization.

SOC 2 Type 2 Report - SOC 2 Report covers the Security, Confidentiality, and Privacy Trust Services Criteria. SOC 2 Report confirms that SysCloud controls are designed and operating effectively to meet the 2017 Trust Services Criteria.

HIPAA

HIPAA refers to the Health Insurance Portability and Accountability Act (1996). HIPAA is intended to protect security and privacy of medical data. There is no official certification for HIPAA. HITRUST is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the Common Security Framework (CSF) which builds on builds on HIPAA and the HITECH

Act. SysCloud leverages on the HITRUST CSF mapping to SOC 2 and is part of the SOC 2 Report.

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law intended to protect the privacy of students' education records, including personally identifiable and directory information. The law applies to schools, school districts, and any other institution that receives funding from the US Department of Education, effectively all public K-12 schools and school districts, as well as most post-secondary institutions, both public and private. SysCloud has performed an assessment and have mapped key compliance requirements of FERPA with the SOC 2 controls and is included in the SOC 2 Report.

COPPA

Children's Online Privacy Protection Act of 1998 (COPPA) is a federal law intended to regulate collection of personal information from children under the age of 13. COPPA imposes various requirements on operators of websites or online services to protect customer information. SysCloud has performed an assessment and have mapped key compliance requirements of COPPA with the SOC 2 controls and is included in the SOC 2 Report.