SKYBRIDGE
BY INSPECTIONLOGIC

Security Policies and Procedures – Fall 2020

The security standards employed by SkyBridge/InspectionLogic will be classified into broad categories of risk/responsibility as follows:

1. Identification and Authentication
2. Logical Access Control
3. Protection against malicious software
4. Software distribution protocols
5. System input /output controls
6. Back-up/storage of data
7. Incident handling
8. Shared responsibility for compliance
9. Vendor staff roles

Identification and Authentication

Users will be identified uniquely ensuring that any action can be attributed to a specific user. This rule applies to the operating system level and to the application level. The following minimum requirements should be satisfied.

- Each user has a unique identity (user ID).
- A list of users and their unique identities is maintained.
- Each authentication identifier is assigned to a user and is used by a single user.
- Only system administrators have identities that correspond to accounts with elevated privileges and those accounts are only used for tasks that require elevated privileges.
- All server user accounts, and database user accounts will have passwords of at least 50 randomly generated characters consisting of lowercase letters, uppercase letters, numbers, and symbols.
- All server passwords will be stored in a secure password management system, preferably employing an autofill mechanism so that passwords are unknown to vendor staff. No passwords will be written down or transmitted in any form via email, text message or any other electronic means other than assignment into the password management system.

Identification and Authentication, continued

- Passwords and connection strings in management systems, configuration files and security databases will be stored with 256-bit AES encryption ciphers.
- All staff access to web servers and databases will be logged and monitored
- All support staff access to databases for the purposes of user support, data conversions, data remediation, etc. will require written approval, via email from an approved customer representative using an enterprise domain account, to be presented by the supporting party to a SkyBridge security administrator who will control and monitor their access.
- All access to any portion of the SkyBridge infrastructure and data will be done via pre-authorized and pre-configured, encrypted VPN connections from predefined static IP addresses assigned to the specific individuals requiring access. Firewall rules enabling this access are to be temporary and to exist only for the life of the approved access.
- All data traffic between SkyBridge servers will occur on a private virtual network within the Azure backbone. No traffic will flow over the public network between SkyBridge servers, and databases.
- All traffic to, from, or between end user devices and web browsers will be SSL encrypted with third party certificates.

Logical Access Control

- There will be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.
- Registered user accounts shall be reviewed for applicability at specific periods.
- Privileges shall be defined for specific business purposes.
- The allocation and use of privileges will be restricted and controlled.
- Privileges and privilege allocation shall be reviewed for applicability at specified periods.
- The allocation and establishment of user passwords shall be controlled through a formal management process.
- Management shall review user rights at regular intervals using a formal process.
- Users are required to follow good security practices in the selection and use of passwords.
- All support staff access to applications, servers and data will be via monitored Azure Active Directory user accounts within a dedicated domain designated for SkyBridge DevOps and Support activities.

Protection against malicious software

- Special care should be taken to control the development and maintenance of software applications.
- Application development should be conducted with specific, scientifically accepted methodologies. (i.e. Agile SCRUM and Microsoft Best Practices for Azure and SQL Server)
- All third-party libraries, controls and components will be purchased from recognized major software houses with proven track records for security, support and reliability. All second- and third-party code libraries will be loaded and maintained from well known, approved and documented NuGet package repositories.
- Each new application feature must be accompanied by documentation.
- The risk analysis must fit into the requirements analysis.
- Systems utilized for the development and testing of software must be separate from the operational systems.
- Software changes should be authorized prior to their implementation:
- Any change should be examined for its effects on the security of the information system.
- Changes that affect security requirements must be approved by the Security Officer.
- Code changes and updates must be made in the development/testing environment and should be tested prior to their application to the operational system.
- All code, libraries, assemblies, scripts and digital assets deployed will be subjected to virus scanning software and Azure Security Center real time monitoring for threats and vulnerabilities.
- All software changes must be accompanied by documentation updates. (change logs) Change logs are to be submitted to, approved by and maintained by non-developer support personnel.
- In cases where urgent changes are required, it is necessary to ensure the following:
    - Keep to a minimum the changes that will be performed.
    - The modified files must be monitored.
    - The Security Officer must be informed.
    - Irrespectively of how urgent the modifications are, they must be tested before they are incorporated in the live system.

  After any kind of modifications on the live system it is necessary to re-test system security. To this end the Security Officer must monitor the effectiveness of the security mechanisms after the modification took place. Automatic security testing will occur daily when appropriate and no less weekly.

Secure Data Management

- Data should be categorized according to the protection they need, as derived from the risk analysis or assessment of the Security Officer.
- The following categories have been identified:
    - Top secret: information and critical data of the Information System that any disclosure or unauthorized modification will have direct impacts on the operation. (e.g. connection strings, passwords, server access codes and procedures, etc.)
    - Confidential: information and data that is important for seamless operation and should be subject to strict controls and protected. (e.g. End user identifying information and codes)
    - Sensitive: information and data that is subject to legislation on protection of personal data. Disclosure of this data requires specific permission / license. (e.g. User and customer owned data)
    - Reportable: information and data that can be disclosed. (e.g. User notifications, regulatory notices, etc.)

        The requirements of information security and the way data is processed vary according to the category of information. It is necessary to specify the authorized data recipients, according to the above classification. Data processing must ensure procedural and technical resources that can be attributed to a specific individual. Therefore, all critical operations will be accessed in a strictly personalized way.

Back-up and storage of data

User and/or site data will be backed up on an automated schedule.
Backup data will be stored at data centers that are geographically remote from the production data. (i.e. "offsite")
Backups will be maintained for appropriate periods, *typically daily, monthly and annual backup sets*. (Customers must apprise InspectionLogic in writing of any unique retention policies or regulations that they wish to apply to specific sites or databases.)
Vendor will not employ hybrid data storage schemes. No customer data will be stored in or backed up on vendor's private networks or computers. All customer data will always reside inside Microsoft Azure data centers or other qualified Infrastructure as a Service (IaaS) provider data centers.

Recording of actions and events, and intrusion prevention

Note: The following rules are programmatically applied (to the extent possible) by an Azure Security Center service.

- Incidents of failure or non-routine functions of hardware or/and software should be recorded and evaluated in relation to the operation that they support.
- Critical application systems should exhibit real time alarm systems.
- If there is a risk of invasion by external systems, intrusion detection and prevention systems should be in place.
- Systems will record the suspicious actions for the invasion and react automatically if this is dangerous for the security of the Cloud Provider.
- Proven invasions activate alarm system in real-time.
- The log files should be protected from loss or intentional corruption.
- The logswill be inspected by authorized personnel from time to time to highlight events / actions that endangered the Service Provider.
- Real time alerts to DevOps and the Security Officer will be utilized to report potential vulnerabilities and threats whenever possible.
- The exercise of rights of access users will be monitored and controlled in order to avoid the abuse of rights.

Compliance with regulatory requirements

- It is necessary to comply with existing legal and regulatory framework.
- We will comply with legal obligations for use of hardware / software, i.e. the necessary licenses.
- We will employ appropriate and reasonable measures for protecting critical data from loss, destruction and unauthorized amendment in accordance with legislative requirements.
- We will employ appropriate and reasonable measures to ensure data protection and privacy as required by laws and regulations.
- We will monitor and comply with relevant technical standards and practices of software development.

Protection of surveillance systems

- Access to system monitoring and logging tools will be controlled.
- Access to the monitoring tools will be restricted to authorized persons.
- Restrict the access rights of the administrators in order to ensure that they will not be able to remove or change log details of their own actions.
- In order to facilitate reliable, auditable monitoring and logging, the clocks of different systems must be synchronized.

Supervision and control

Note: The following rules are programmatically applied (to the extent possible) by an automated Azure Security Center service, and/or, as part of Windows Server™ Event Logging and Group Policy settings that are also monitored by an automated security service.

- Audit trails and event logs must be recorded in order to support the identification of violations or attempted violations and scrutinizing every suspicious incident.
- Maintenance of monitoring data for all systems supporting multi-user access.
- Record the use of privileged functions.
- Record system startup and shutdown.
- Record failed attempts.
- Record log-on/log-off events
- Record changes in access rights and use.
- Record the basic data for each suspected case.
- Record the user identifiers (User IDs).
- Record the time and the time of the event.
- Record the type of the event.
- Record the files accessed.
- Record the identity of the user.
- A copy of the audit data files must be kept in back up media (back-up).
- Access to log files is prohibited in those that do not have privileges (administrative rights).
- Log files should be protected from potential disaster.
- There should be integrity checks in place.
- Log files should be tested at least once a year.
- If the space available for log files approaches storage capacity, an alarm must be produced.
- Periodically analyze logs of actions and events.
- Monitor the creation of accounts with elevated permissions.
- Identify deviations from normal use of system resources (e.g. excessive exporting or reporting activities, excessive logins or logins from unusual locations).
- The system automatically notifies the Security Officer when it detects certain suspicious events.

Shared responsibility for compliance

Cloud security is a shared responsibility between the cloud vendor and its customers.

SkyBridge customers, their employees and assignees, contractors, and field technicians are responsible for taking reasonable care by taking a holistic view of their data protection and compliance posture when either they or their representatives are using SkyBridge cloud services. Customers should perform their own risk assessments and codify their compliance rules and processes by providing recommended actions, evidence gathering, and audit preparedness. Customers should understand the division of responsibility between their enterprise and InspectionLogic/SkyBridge in a SaaS deployment. Customer employees and representatives will have a level of access and control appropriate to their roles as described by the customer enterprise. This may include the ability to view, modify, export, expose and/or erase data that belongs to their organization.

Vendor does not own the customer data or assume responsibility for how customers use the applications or data. As such, customer enterprises are responsible for security that would prevent and minimize the risk of malicious data exfiltration, accidental exposure, or malware insertion.

Reporting and data retention regulatory responsibility remains with the customer. Customer may contact a vendor representative or support team member if they need assistance saving, exporting, or reporting data or for assistance with other regulatory agency compliance issues.

Regardless of the platform holding the data (SaaS or on-premises), the enterprise customer will always be responsible for ensuring the security of its own data.

Customer is responsible for reviewing and understanding the EULA that was provided to them when they entered into the SaaS agreement.

Vendor staff roles

Vendor staff will be assigned to various group classifications to promote separation of responsibilities to the extent that it is practical and judicious to do so. The major role divisions will be:

- Application Support
- Application Development
- Database Administrator
- DevOps Support
- Security Officer

References

Georgiou, Dimitra & Lambrinoudakis, Costas. (2014).

"A Security Policy for Cloud Providers, The Software-as-a-Service Model. 10.13140/2.1.2891.6489. Cloud Computing is a new computing paradigm originating and combining characteristics from grid computing, distributed computing, parallel computing, virtualization and other computer technologies. Trust and security in Cloud Computing are more complex than in traditional IT systems. Conventional security policies designed for other technologies do not map well to the cloud environment, which, on top of that, may exhibit additional security requirements. In an attempt to assist cloud providers to secure their environment, and specifically for the Software-as-a-Service Model (SaaS), this paper starts with the presentation of the already reported threats. Because of these security threats, there are specific requirements that we claim must be clearly addressed in the Security Policy for the Cloud Environment. Our work focuses on the required structure and contents of such a security policy. In this respect, this paper proposes a model to describe the relationship between threats, measures, and security policies applicable to the SaaS model. It is worth stressing that in the SaaS service model, the client depends on the provider for the proper security measures."

Security best practices for Azure solutions - Microsoft

Published: 4/19/2019

"This paper is a collection of security best practices to use when you're designing, deploying, and managing your cloud solutions by using Azure. These best practices come from our experience with Azure security and the experiences of customers like you.

This paper is intended to be a resource for IT pros. This might include designers, architects, developers, and testers who build and deploy secure Azure solutions."