Security Policy

Version 2024-11-05

- Introduction
  - Purpose and Scope of this policy
  - Policy updates
  - Roles and Responsibilities
    - Keep Everyone Secure
    - General Circle
    - Multi-circle roles and KES
  - Exceptions
  - Definitions
- Artificial Intelligence
  - AI software assessment
  - AI software inventory
  - AI Usage Policy
- Asset Management
  - Asset Inventory
  - Asset reporting duty
- Cloud Security
  - Cloud & Responsibility model
  - Cloud provider security
- Configuration Management
- Data Classification and Handling
  - Data Classification
  - Data handling rules
  - Data Inventory
  - Paper policy
  - Transfer of credentials and sensitive personal information
- Endpoint Security
  - Authorised endpoints
  - Computer policy
  - Mobile Device policy
  - Endpoint security software
  - Endpoint security review
  - Endpoint lifecycle management
- Human Resources Security
  - Background checks
  - Onboarding
  - Offboarding
- Identification & Authentication
  - Identification methods and Single sign-on

- Account creation
- Authentication methods
- Password policy
- Credentials and secrets management
- Access management

Incident Response
- Inappropriate data disclosure process
- Incident management
- Loss or compromise of a Team Member asset

Network Security

Physical & Environmental Security
- Travel

Risk Management
- Incident review

Security Awareness & Training

Security Operations
- Problem tracking and auditing
- Escalation & emergency handling

Secure Engineering & Architecture
- Secure Baseline Configurations
  - Encryption of customer data (data-at-rest)
- Vulnerability & Patch Management

Other
- Review of core operating systems and application systems

Policy History

Introduction

Purpose and Scope of this policy

The Skyscrapers Security Policy defines all security practices within Skyscrapers (the trade name of "ILIBRIS BV") that are needed to deliver services to our customers and operate the business in a secure way. It is to be followed by any party that has access to Skyscrapers information and systems, customer environments and customer data.

Skyscrapers currently has no formal certification for any Information Security Management System (ISMS) like ISO27001, NIST, etc. However we try to align all improvements and implementations to such formal ISMS's. This makes us a better company and it will make it easy to eventually move to get formally certified.

Policy updates

This Security Policy is regularly updated following for example: new insights, new identified needs in the organisation, third party input and identified security risks to be controlled.

All changes and major milestones are tracked in the History section. Additionally all changes since the previous version are marked.

We use the following process:

1. Potential updates and changes are collected by KES on an internal backlog.
2. KES determines when the time comes to publish an updated version and decides what to include for that version.
3. KES creates a new version draft.
4. Skyscrapers teams are requested to review the draft and provide feedback and comments.
5. KES processes this feedback and produces a final version.
6. When the KES team unanimously approves the final version it is published.
7. The new version is published internally and towards all customers.

Roles and Responsibilities

Keep Everyone Secure

This document and the underlying policy is owned by a dedicated team called "**Keep Everyone Secure**" ("**KES**"). It has the following aim:

> *Develop, implement, maintain and communicate clear and unified security practices and standards and be first contact for all security matters.*

This team has full authority over:

- Security practices and standards for internal working, products and services
- Training and support of the organisation around security
- Legal compliance implementation
- Disaster Recovery/Business Continuity for Skyscrapers

This team meets regularly to review the current state of security and actively improve it. All activities and decisions of this team are logged.

This document is owned by the KES team.

General Circle

Skyscrapers has a central management team, called the **General Circle ("GC")** that holds the responsibility for delivering the Skyscrapers strategy, corresponding services and supporting processes. In the scope of this Security Policy the General Circle has a consultative role where KES needs to request a review by GC before publishing a new version of the Security Policy.

Multi-circle roles and KES

Due to the unique organisational nature of Skyscrapers, people can hold roles in multiple circles[1] with conflicting interests. For example: a person could hold an operational role doing hiring/HR but can at the same time also be a member of KES. If that person would need advice on how to approach security for a new hire, this person would potentially respond to him/herself.

To mitigate this potential conflict-of-interest, the following rules must be followed:

1. For all requests from a person that is a member in both the requesting circle and KES, the request must be handled by another member of KES that has no direct conflict of interest.
2. All important decisions impacting organisational security need consent from ALL members of KES. This consent needs to be logged.
3. In case the above rules cannot be followed for practical reasons, a deviation is acceptable under the condition that the General Circle is informed.

Exceptions

There may be use-cases related to professional activities or other unforeseen situations that require deviations from this policy. Such exceptions need to be requested from KES. KES will analyse the motivation, the risks and proposed controls to ensure information security is maintained. If deemed acceptable KES will approve the exception.

All exceptions are tracked to allow for ongoing evaluation.

Definitions

Company Resources: composed of all systems that Skyscrapers maintains and uses to perform any of its activities, all personal and confidential information living in those systems, all Customer Infrastructure and Customer Data we potentially have access to.

Customer Infrastructure is the computing infrastructure (compute, storage, networking, etc) sourced from a cloud provider by the customer, on which Skyscrapers performs Services. On top of this Customer Infrastructure the Customer may deploy Customer Applications and Customer Data may be processed.

Customer Data: any form of data that is owned by the customer and is accessible through Customer Infrastructure. This includes but is not limited to company data, commercial information, Personal Data of its customers, etc.

[1] In Skyscrapers "circles" are a concept similar to "teams" in many other organisations.

Data in the scope of this documentation is all kinds of data and information.

Personal Data: any information that relates to an identified or identifiable living individual according to the GDPR.

Personnel are all people on the payroll of Skyscrapers, either through an employee contract or through an independent-contractor contract (self-employed contractors), that act as individually identifiable people within the Skyscrapers team.

Skyscrapers Applications: systems and applications holding only internal 'business' information of Skyscrapers. This includes internal chat, email, calendar, CRM, on-call information, commercial documents and other internal administrative information. This definition expressly excludes Skyscrapers Infrastructure.

Skyscrapers Infrastructure: software, systems and cloud environments that Skyscrapers uses for internal purposes (Development, operations, etc) that may or may not provide access, directly or indirectly, to Customer Infrastructure and/or Customer Data.

Team Member is a person that works for Skyscrapers as part of Personnel. In plural ("Team Members") this means all Team Members.

Artificial Intelligence

AI software assessment

Before a new AI software is taken into use in Skyscrapers, a review will be conducted:

1. Will the input data be used in training of general AI models?
2. Is there a DPA in place between the vendor and Skyscrapers?
3. Who has access to the input data?
4. How long will data be stored?
5. Where is the data stored?
6. What security measures are in place

The above information will be evaluated by KES and approve or disapprove the usage of the AI software in Skyscrapers. In case it is approved, additional usage limits may be imposed.

All assessments, conclusions and approvals will be maintained in a central registry which can be found in the AI software inventory.

AI software inventory

Skyscrapers maintains an AI software inventory that stores the results of the assessments and tracks the usage of AI software in Skyscrapers. It is maintained by KES and can be found here:
KES Asset, AI and Data Inventory (Restricted).

AI Usage Policy

Usage of software that offer Artificial Intelligence (AI) functionality by any Team Member is allowed respecting the following rules:

1. When a Team Member wants to start using AI, the AI software inventory needs to be consulted to see if the AI software is approved, not approved or unlisted.
    a. not approved: you are not allowed to use the software for Skyscrapers
    b. pre-approved: KES needs to be informed of your intent and what for (purpose)
    c. new, unlisted AI software: request permission from KES, who will do a review first (cfr. AI software assessment)
2. Care must be taken that rules on Data Handling, confidentiality and data privacy are respected (e.g. be careful with AI software implemented as a browser extension).
3. No Customer Data is ever uploaded to or processed by AI tools

Asset Management

Asset Inventory

Skyscrapers maintains an inventory of all hardware, software and cloud assets associated with Data and Data processing facilities used ("Asset Inventory"). That inventory also lists who is the individual that is responsible for that asset.
The Asset Inventory can be found here: KES Asset, AI and Data Inventory (Restricted).

Asset reporting duty

Team Members must keep KES up to date regarding all assets that may start holding Data or start processing Data in the context of Skyscrapers' activities. This includes:

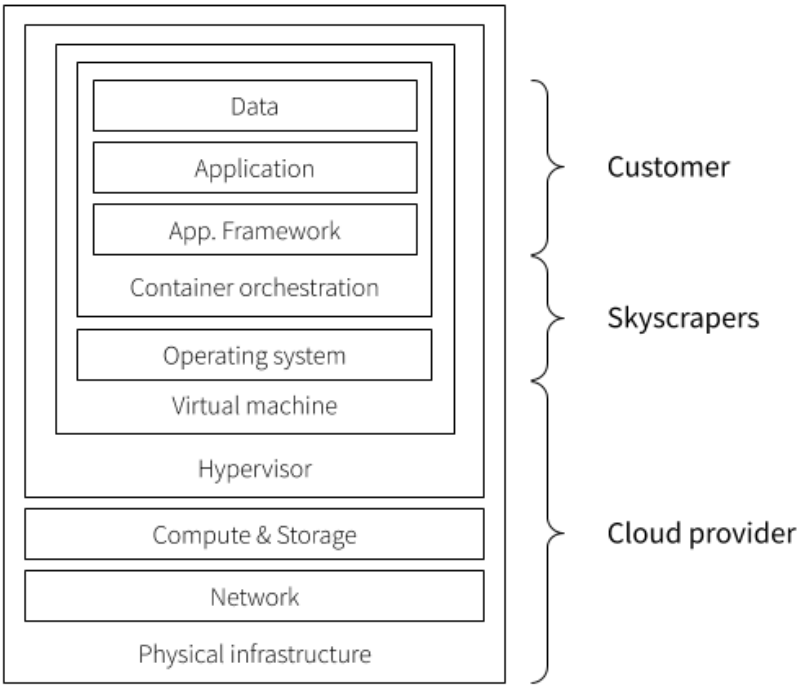
- Introduction of new assets (new computers, new mobiles phones, new SaaS tools, etc.)
- Stop of processing by these assets
- Compromise (hack, loss, etc.) of any of these assets (cfr. Incident Response)

Cloud Security

Cloud & Responsibility model

Skyscrapers does not manage any physical hosting infrastructure: we operate as a cloud-broker using the services of public cloud providers. See **Cloud provider security** for their respective Security Policies.

An application stack is composed of multiple layers. The following is a simplified representation of the various responsibilities over each layer:



Cloud provider security

Each cloud provider has their own security policies and resources.

Amazon Web Services

- AWS Cloud Security
- AWS Privacy
- AWS Cloud Compliance
- AWS GDPR Center

Microsoft Azure

- Azure compliance documentation
- Azure Service-level Agreements
- Azure compliance documentation
- Azure ISO27001 compliance

Configuration Management

All Customer Infrastructure built and managed by Skyscrapers is orchestrated in an automated and codified way. We use such tools as GitHub, Terraform, Concourse CI and other systems for that. This ensures:

- tracking of changes (who, time, etc)
- repeatability
- limitation of room for human error

All updates to the configuration management system are versioned in GitHub repositories. Customer specific configurations are versioned in private repositories. This ensures all changes are recorded

and traceable.

Depending on the version of the customer's specific hosting stack, the level of coverage of configuration management may vary. Older systems tend to still have partial manual management, thus not offering all the advantages mentioned above.

Data Classification and Handling

Skyscrapers classifies information, data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. This also allows for determining how to best handle that date throughout its lifecycle.

Data Classification

We identify the following classes for all information:

Public
This information and data is publicly shareable. It is expected it does not expose Skyscrapers or its customers to any harm or material impact.
Examples: public changelog, public documentation.

Restricted
Data and information that is created and used in the normal course of business and that can not be made publicly available. It is by default shared with all Team Members. Depending on the requirements of a specific cooperation it may be shared with specific audiences like a customer or a partner as well, providing the necessary requirements for sharing such data are met.
Unauthorised access or disclosure could cause minimal risk or harm and/or adversely impact Skyscrapers, its partners, Team Members, contractors and customers.
Examples: Flight Manual (internal processes), customer specific documentation, customer repositories, information about customers, etc.

Confidential
Very sensitive data and access that is considered privileged and must be explicitly approved by the data owner(s).
Exposure of this data to unauthorised parties could cause privacy violations or cause significant commercial or legal damage to the business of Skyscrapers.
Examples: scans of personal IDs and passports

Customer Data
Data that must never be handled or shared with anybody, not even to Skyscrapers members, except in exceptional cases with approval from the data owner (the customer).
Exposure or misuse of this data could cause significant commercial or legal damage to Skyscrapers and its customer(s).
Examples: Customer Data like data stored in databases that we manage, etc

Data handling rules

Credentials and access tokens are classified at the same level as the data they protect: this means credentials such as passwords, personal access tokens, encryption keys, and session cookies derive their

classification from the highest classification of the data they protect.

Combinations of data types may result in a higher system classification level: If there is more than one data type residing in a system, the system should be classified at the highest data classification level of the data being stored, transmitted or processed on that system.

Confidential data must be labelled: if data is of the Confidential class, it needs to be clearly labelled as such.

Customer Data must never be accessed by Team Members, unless in exceptional circumstances with explicit written approval and instructions from the Customer.

Data owners classify: Data owners are responsible for assigning the correct classification and for identifying any additional requirements for specific data or exceptions to standard handling requirements. KES offers guidance where requested or needed.

Labelling is advised: Except for Confidential data, labelling data and information according to this policy is not required. However, labels are still encouraged. By labelling data according to classification levels, individuals can quickly refer to this policy for proper handling.

Data Inventory

Classification of our actual information, data and assets is tracked in the Data Inventory which can be found here: KES Asset, AI and Data Inventory (Restricted). All Data owners are responsible for maintaining consistency with this Data Inventory.

Paper policy

Paper is allowed, but the following guidelines must be kept in mind:

- Depending on the data classification, store the information in a secure place to maintain the right level of confidentiality.
- Destroy the paper once it no longer serves a purpose.
- When destroying paper, make sure the information on it is completely destroyed and unretrievable.

Transfer of credentials and sensitive personal information

Credentials can be any of the following:

- Credentials (username/password)
- SSH keys (private)
- SSL/TLS keys (private)
- VPN profiles (private)
- Tokens
- Personal Data like bank account numbers, passport ID's, etc.

These are only communicated using guaranteed encrypted and private communication channels like keybase.io and cyph.app. Slack is not considered secure enough for this data.

Endpoint Security

Authorised endpoints

Any machine used by a Team Member to access Company Resources is called an Endpoint. The following rules must be followed:

- Any access to Company Resources needs to be done from a registered hardware asset (cfr. Asset Management).
- Never access Company Resources or data from a **public or shared device.**
- Team Members must report any suspected misuse or theft of any device or token (hardware/software) used for accessing Company Resources, immediately to KES (cfr. Incident Response).

These Endpoints can be company owned or self-owned. In either case Endpoints can be used for both Skyscrapers usage and personal usage, as long as all security requirements from this policy are adhered to. In case these standards are not compatible with personal use, a dual boot configuration is an acceptable solution (using separate disk encryption on both volumes is required).

Computer policy

This covers computers (fixed, laptop) that are typically used to perform regular working activities using any Company Resources, other than Mobile devices.

These must adhere to the following security standards:

1. Skyscrapers endpoint client software is required to be installed and correctly functioning
2. No remote access to the machine is allowed
3. Lock computer:
    a. Trusted location after 10 minutes or sooner
    b. Untrusted location always lock immediately
4. All storage must be encrypted
5. Computer users: no anonymous guest users, no unauthenticated accounts
6. Super-user or root accounts must not be interactive
7. Only correctly licensed software must be installed on the machine
8. No illegal or other potentially security-harming activities can be performed on the machine
9. Operating Systems (OS) choice is free as long as Skyscrapers provided security software (CrowdStrike, Kolide) and other software tooling needed to do work are 100% functional and the security policy can be fully respected
10. The OS and all installed software must be an actively maintained version and be kept up to date
11. System level and user level passwords must, where applicable, adhere to the Password policy
12. General caution and risk awareness has to be top of mind (opening email attachments, etc)

Mobile Device policy

This covers devices other than full computers, like phones, tablets, etc that may be used to access and have access to Skyscrapers Applications.

Mobile devices used for accessing Skyscrapers systems must, at least, adhere to the following security standards:

1. Require authentication (secure PIN, pattern or biometric authentication)
2. Lock device:
    a. Trusted location after 10 minutes or sooner
    b. Untrusted location always lock immediately
3. Up to date and actively maintained operating system
4. No cracked or jailbroken device or software
5. Only have applications installed from trustworthy sources approved by the mobile device vendor
6. No illegal or other potentially security-harming activities can be performed on the device
7. Any mobile device used to access company information must not be shared with any other person. The only exception to this is direct family members under supervision of the device owner.
8. Upon termination of the Skyscrapers cooperation the Skyscrapers Members must to return all company owned devices and delete all company information and accounts from any personal devices

With the above implemented the following is expressly not permitted:

1. Mobile devices or any of the installed applications **cannot** be used for accessing Customer Infrastructure, directly or indirectly.

The following applications and/or websites are expressly permitted for accessing Skyscrapers Applications:

1. Google Workspace: Mail, Calendar, Drive
2. Slack
3. Zoom
4. Notion
5. Opsgenie
6. Twilio voicemail
7. GitHub for tracking issues, reviewing Pull Requests and reading documentation. However it is not permitted for performing unreviewed code updates (through GitHub or other tools).

In case you want to use **other applications** to access Skyscrapers Applications, you are welcome to do so as long as:

1. the requirements under this section are fully met
2. you notify KES of the application and its intended usage

Endpoint security software

Skyscrapers rolls out the following client software to all computer endpoints:

- Kolide for security & compliance reporting and tracking of endpoints
- CrowdStrike Falcon as EDR for active and intelligent threat detection and response on endpoints

These clients are rolled out and followed up by the KES team and supported by an external security service provider. Only KES and this service provider have access to the global security view these tools provide.

Whenever possible and within the limits of ensuring security, Team Member privacy will be maximised in client collection and reporting capabilities.

Endpoint security review

The KES team reviews the current state of Kolide and Crowdstrike, including the recent alerts on a bi-weekly basis. Based on that follow-up actions are determined both for short term and long term (e.g. monitoring adjustments, implementation of controls, policy changes, etc).

Endpoint lifecycle management

1. All computer endpoints used for working with Company Resources are to be reported to KES.
2. When computer endpoints are taken out of service, we require all Company Resources, and access to these, to be removed. KES tracks this and provides guidance for this.

Human Resources Security

Background checks

When hiring new Team Members, the following is verified to be in line with information provided upon application:

1. The professional references by contacting at least 2 colleagues from the past
2. Social media networks where available
3. The personal ID

Onboarding

When new Team Members start in Skyscrapers a formal onboarding process is started. From a security point of view this includes:

1. Ensuring endpoints are secured appropriately
2. Security training
3. General introduction to company processes and structures
4. Phased access to systems

Offboarding

When a Team Member leaves the company, an offboarding process is started. From a security point-of-view this includes:

1. Removal of all access the ex-Team Member has
2. Request for formal confirmation of removal of all Skyscrapers Data from their (self-managed) endpoints and systems (Skyscrapers provides guidance for doing so).
3. Ex-Team Member returns all company owned devices

Identification & Authentication

Identification methods and Single sign-on

Skyscrapers maintains two central methods for user identification for all Personnel:

1. Google Workspace (formerly known as “Google G Suite”)

2. Github Teams

Both services are configured according to the Authentication methods policy and serve as the primary identification service for Single sign-on ("SSO") services.

For accessing any application or system the following method for identification must be used, in order of preference:

1. Whenever possible one of the two central identification methods (Google Workspace or Github Teams) must be used as an SSO method for identification to the respective service.
2. If no SSO is available, a new individualised user account must be created on the system respecting the methods lined out in the Authentication methods policy.

In all cases and at all times:

1. The Access management policy must be followed.
2. Individualised user accounts must be used for auditing and security reasons. ❗ Exceptions can be handled by the Exceptions process.

Account creation

Whenever new accounts are created for Skyscrapers' purposes and using SSO is not a possibility, a personal Skyscrapers email address (<team_member>@skyscrapers.eu) must be used. Exceptions can be made with approval from KES.

Authentication methods

We always default to the most secure access method available, depending on what the tool or service supports. In order of preference:

1. Passkeys (WebAuthn/FIDO2 authentication). This includes those provided by:
    a. the Skyscrapers password manager (1Password)
    b. your OS, using biometric unlocking
    c. a hardware token, like YubiKey, provided a PIN is configured
2. 2FA (two factor authentication) using as a second factor a hardware or biometric token
3. 2FA using as a second factor a software generated TOTP, like provided by 1Password
4. ❗ In all other cases an exception needs to be requested

In case systems or services support public/private key pair authentication, this is required over using a password. The private key in that case must be protected with a password.

Password policy

This applies to all accounts on systems, services and devices accessing or touching Company Resources.

General guidelines

- New devices, installations and software deployments must have default passwords either be disabled or set anew.
- Passwords must be different and unique across all services, devices and accounts. Usage of a random password generator, like 1Password, is strongly advised.
- Passwords must not be written down or viewable by anybody else in any other way.

- Passwords must, if possible, be at least 14 characters long and be a mix of letters, numbers and symbols. In case a system prevents this, use the most secure mix available for that system. Usage of a random password generator, like 1Password, is preferred.

In relation to Company Resources (and Skyscrapers Applications):

- Personal and shared passwords that are needed for accessing Company Resources have to be stored in the Skyscrapers provided password manager (1Password).
- Usage of strong biometric authentication for accessing passwords is advised and permitted.

Credentials and secrets management

For personal credential management:

- 1Password: Skyscrapers provides a company-wide business licence to 1Password to store, manage and share personal and shared credentials. 1Password has built-in checks for breach detection.
- Aws-vault: for managing encrypted AWS account credentials using the OS keyring.

For shared credentials (not preferred, see below) the team functionality of 1Password is to be used.

Store 1Password access credentials according to their best practices:

- https://support.1password.com/secret-key-security/
- https://blog.1password.com/where-to-store-your-emergency-kit/

Access management

All new Team Member-level access to Company Resources is to be notified to and approved by KES. The Team Member can do this using the Slack Workflow “Request access“, available in the *#team* channel.

When accessing Company Resources, it’s required to always start from the minimum privileged role needed to be able to start on the task being executed. Only escalate to higher privileges for the parts of the task that require it, thus limiting the security risk.

Incident Response

Inappropriate data disclosure process

The following process is the standard at Skyscrapers when we are notified or detect an inappropriate data disclosure:

1. Isolation of the potentially vulnerable application and/or dataset. This might incur unscheduled downtime.
2. Inform the customer that owns the platform to plan and decide next steps.
3. Investigate cause and/or vulnerability. Depending on the risks presented, appropriate corrective actions are taken. Worst case this can include a complete rebuild of the environment.

These processes follow commitments of the service level agreement chosen between Skyscrapers and the customer.

Incident management

We have a team-wide Incident Reporting process using automated Slack workflows. Each reported incident gets inventorized and rated by probability, availability impact, data impact and affected customers. This is done by KES, a dedicated security circle (team).

The incident inventory gets regularly reviewed (at least bi-weekly) to provide possible mitigations and controls for each Incident.

Loss or compromise of a Team Member asset

Whenever an asset of a Team Member is compromised (hacked, credentials leaked, etc.) or lost:

1. The asset, if possible, needs to be taken out of use and all access to Company Resources needs to be revoked ASAP.
2. An incident needs to be logged to KES describing what happened and mitigation steps were taken.
3. KES will log and follow-up further.

Network Security

Considering the fact Skyscrapers is a fully remote team and working directly in the cloud, regardless of location, **all work for Skyscrapers is required to be done over encrypted connections**. This includes but is not limited to TLS, web over HTTPS, SSH, IPSec, etc.

Any client encryption and VPN software used to set up such secure channels needs to be approved by Skyscrapers. Today only the following solutions provided by Skyscrapers are approved (“Skyscrapers Provided VPN”):

- Tailscale via our production environment

Access and any traffic to Customer Infrastructure requires use of the Skyscrapers Provided VPN

Use of public Wi-Fi (including those with captive portals) for accessing Company Resources is not permitted. In case no other option is available, the use of Skyscrapers Provided VPN is required for ALL traffic.

Physical & Environmental Security

Skyscrapers has a distributed working setup. There is a formal central office that serves as administrative HQ and supports occasional team and customer meetings. 100% of the time we work remote. This can be from home, co-working spaces or other suitable locations.

In that context the necessary security precautions have been taken, depending on the type of location:

1. **Trusted Locations**: a permanent home, office or coworking location that is formally registered with Skyscrapers.
2. **Untrusted Locations**: Any other place not listed as “Trusted Location”, like public places, customer locations, hotels, friend’s houses, etc.

Working from **Untrusted Locations** is ok, but requires strict adherence to security standards and additional vigilance, for example:

- Always check for cameras and face away screen and keyboard from any that may be present.
- Sensitive conversations in the same physical location, both internal and with customers, are done in closed rooms so no eavesdropping can occur.

Travel

Team Members are required to notify KES when travelling abroad while still working for Skyscrapers and accessing Company Resources from outside their registered country. The KES team will evaluate and log an exception when permission is granted.

Risk Management

Incident review

The KES team reviews all (non-urgent) registered risks and incidents (see Incident Response) on a regular basis. All newly registered incidents and risks are categorised according to severity, business impact, chance of happening and data exposure. Based on that follow-up actions are determined both for short term and long term (e.g. implementation of controls, policy changes, etc).

Security Awareness & Training

Our team considers security as a constant throughout everything we do. We follow all industry best practices and improve when weaknesses are exposed. This is also manifested during the mentoring period of newly hired Team Members.

This Security Policy is an integral part of the Skyscrapers Flight Manual. This is a collection of documents that covers topics like processes, operational guidelines, core values, etc. Therefore it is expected to be known and understood by everybody on the team.

Every 6 months we organise a Security Training covering all topics related to security: GDPR, Security Policy, the Incident Process and any recent updates to these.

Security Operations

Problem tracking and auditing

Skyscrapers maintains a work-tracking system to track all customer requests, problems and incidents. This system ensures adequate follow-up, coordination across the team over time and auditing.

Escalation & emergency handling

Skyscrapers has internal escalation processes for managing customer escalations, incidents and

systems alerts generated through our monitoring.

Secure Engineering & Architecture

This section applies to all cloud-solutions and architectures we build and maintain for customers.

Secure Baseline Configurations

Encryption of customer data (data-at-rest)

Providing the chosen technologies supports it, data-at-rest can be encrypted. Many commonly used storage components that we provide, come with encryption of data-at-rest by default:

- We set up databases with data-at-rest encryption by default (RDS, ElasticSearch, MongoDB, Neo4j, ...). S3 we usually also enforce encryption. Basically if it can be encrypted at rest, we do so via the AWS KMS keys per service.
- Kubernetes node volumes (EBS) are encrypted by default on our EKS clusters
- We offer by default encrypted Kubernetes PV volumes for stateful applications, however the customer is free to choose non-encrypted volumes.

For encryption of other components or implementation of different encryption standards, we follow customer instructions.

Vulnerability & Patch Management

For all software under our control and management, we have various processes and controls to keep software at the most recent patch level and rectify any known vulnerabilities. These are further described in our Service Level Agreement and Service Definitions.

Other

Review of core operating systems and application systems

We permit our customers to have an independent party review all aspects that we manage for them. This review needs to be done under supervision of our systems operators (this may be at a cost). It is also limited to those parts where the confidentiality of other customers remains guaranteed.

Policy History

Published by KES	Changes
2024-11-05	Amended Policy updates that updates are marked. Updated, clarified Definitions conform in relation to Data Classification and Handling. Moved and rewrote the Artificial Intelligence section Introduced Asset Management + several updates related to this new sections Introduced Data Classification and Handling + several updates related to this new sections Updated Endpoint Security section: - Integration with Asset Management in Authorised endpoints - Re-ordered & clarified Computer Policy Complete rewrite of Human Resources Security Added Account Creation to Identification & Authentication Updated Authentication methods to: - Clarify approved Passkey systems - Remove SSH key encryption (detail) Added least privilege role requirement to Access management Added new Loss or compromise of a Team Member asset to Incident Response Rewrite of Network Security section Vulnerability & Patch Management updated to refer to SLA and service definition where it belongs. First draft: 2024-10-08, reviewed by circles: 2024-10-18, approved by KES: 2024-10-24