Risk and Security Management Plan

Security and Management System

An IT systems security policy is put in place that sets out all the provisions we take in this regard. It is updated every year, at the minimum, or every time there is a major change that has ramifications for its content. The security of our solutions is assured by formal information security management systems.

IT Administrator Leader is responsible for processes and projects associated with the security, in charge of preserving personal data, coordinates the management of security risks and the associated action plans, implements and applies the provisions pertaining to the risks identified.

Risk Management

A formal methodology for risk management is put in place. This is reviewed annually at the minimum, or in the event of a major change. It also concerns personal information and sensitive data (health, payments, etc.). This methodology formalizes the analyses carried out. It identifies threats and vulnerabilities. A plan for handling any risks identified is devised following each analysis. This plan is then implemented within a maximum of 12 months. It documents the analysis in detail and sets out the order of priority for the actions to be taken. Each corrective measure is added to the action plans and is covered by a formal, tracked follow-up, together with a regular review to re-examine its effectiveness.

System and application development policy

Processes for Skyrise developers are set up and documented. These processes contain the principles of secure development and a code review policy (vulnerability detection, error processing, managing access and entry and protecting storage and communications). Code reviews are also carried out on a regular basis; new features are validated prior to launch, tested in a validation environment (where applicable) and rolled out gradually. A distinction is drawn in terms of roles and responsibilities between developers and the persons responsible for launching production.

Monitoring Services and Infrastructures

A monitoring infrastructure is implemented for any of Skyrise services. This has several objectives: to detect production and security incidents; to monitor critical features, with any alerts being escalated to the monitoring system; to inform the persons responsible and trigger the appropriate procedures; to ensure continuity of service in the performance of automated tasks; to ensure the integrity of the resources monitored.

Incident Management

Incident Management policy is used to prevent, detect and solve issues in the service and its management infrastructures. The process includes: a guide for classifying security events; handling security events. These procedures are covered by a continuous improvement process for the monitoring, assessment and overall management of incidents and their corrective actions.

Vulnerability Management

Technological monitoring for new vulnerabilities is carried. These vulnerabilities are identified via: public information sites; alerts from the manufacturers and publishers of the solutions deployed; incidents and observations escalated by our teams, third parties or customers; internal and external vulnerability scans performed on a regular basis; technical audits and code and configuration reviews. If a vulnerability is detected, it is analysed by dedicated teams in order to determine its impact on the systems and the potential operating scenario. Mitigation measures are implemented, where necessary, and a corrective plan is then defined.

General security measures for physical site

Security measures are taken to regulate access to Skyrise rooms: an access permissions policy; cameras located at the entrances and exits to installations, biometric secure access, a motion detection system; burglary prevention systems at the entrances and exits; intrusion detection mechanisms (security guards 24 hours a day and video surveillance); a permanent surveillance centre monitoring when the entrance and exit doors are opened.

Personnel training and awareness

Skyrise personnel are trained in compliance rules for personal data processing. Awareness training in IT system (IS) security is organised for new employees when they join the company; messages about security are regularly sent to all personnel to ensure that employees know how to act in the event of a threat.

Managing Logical Access to Skyrise System

A strict policy of logical access rights management for users - employees is applied. The access rights and authorisations granted to a user or to a system are managed based on a procedure of logging. All employees use nominative user accounts. If a user forgets their password, only IT Department is authorised to reset it. The use of default, generic and anonymous accounts is prohibited, a strict password policy is applied, users use automatic password generators rather than choosing their own passwords, the minimum length for passwords is 8 alphanumeric characters, storing passwords in unencrypted files, on paper or in web browsers is prohibited, the use of local password management software, which has been approved by the security teams, is mandatory. Any remote access to the Skyrise IT system must be via VPN, using a password.

Security for workstations

Protection of standard personnel Skyrise workstations are in place: updates are managed automatically; antivirus software is installed and updated, and regular scans are carried out, there is a procedure for deleting sessions and resetting workstations when employees leave the company.

Logging

A logging policy is in place for the servers and equipment used by Skyrise. Most of logs are backed up and centrally conserved. Logs are consulted and analysed by authorised personnel, in accordance with the authorisation and access management policy.