Ekco Security Measures Overview

Version 2.0

Contents

1. Scope

This document provides an overview of the administrative, physical and technical security controls Ekco employs in order to maintain the confidentiality, integrity, and availability of its services.

Ekco employs ISO 27001 as the baseline for its services security program. Ekco seeks to continually strengthen and improve its security practices, and so reserves the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of services.

2. Security Program and Policy Framework

Ekco has an ISO 27001 certified security program and policy framework that is established and approved by Ekco's senior and executive management representing various business areas throughout the company.

2.1 Security Risk Management

Ekco utilises a security risk management program that identifies potential threats to Ekco services and infrastructure, rates the significance of the risks associated with those threats, develops risk mitigation strategies, and partners with Ekco's engineering teams to implement those strategies.

2.2 Information Security

Ekco information security is underpinned by our ISO 27001 certified policies and processes. Ekco has appointed a Chief Information Officer (CIO), who is responsible for security oversight and policy strategy, compliance and enforcement. The CIO leads the incident response process, including investigation, containment and remediation of security matters.

2.3 Physical and Environmental Security

Physical and environmental security are key considerations of our ISO 27001 certification. Ekco priorities physical and environmental security and ensures our partners, facility management operations, and staff at all levels maintain the integrity of the physical access to Ekco facilities.

3. Access Control

Ekco operates an ISO 27001 compliant Access Control Policy which requires the use of access control measures designed to ensure appropriate privileges are assigned and maintained for access to company systems, assets, data, and facilities in order to protect against potential damage, compromise, or loss. Ekco follows the Least Privilege Principle, or role-based security, limiting user's access to only what is necessary to perform job functions or roles.

3.1 New Accounts, Roles, and Access Requests

Ekco requires a formal request for access to company systems or data. Each access request requires a minimum approval of the user's manager to confirm the user's role requires access. Access administrators confirm that necessary approvals are obtained prior to granting access to systems or data.

Managers design roles to provide adequate segregation of duties, distributing tasks and privileges among multiple people in order to safeguard information security and to help prevent fraud and error.

3.2 Account Review

Ekco maintains and updates a record of access privileges for employees and contractors authorised to access Ekco systems containing sensitive data.

Ekco performs regular reviews of user accounts and assigned permissions for key systems. Any changes required as a result of the reviews are subject to a formal access request process to confirm the user and the user's role requires access to the relevant system(s). The principle of least-privilege is always applied.

3.3 Account, Role, and Access Removal

Ekco requires user access be disabled, revoked, or removed promptly upon notification of a user's role change (if applicable), termination, user's conclusion of engagement, or departure from the company.

Access removal requests are documented and tracked.

3.4 Credentials

Ekco requires multi-factor authentication for remote access to systems by employees, and enforces our ISO 27001 accredited Access Control and Password Policies which include the following password handling and management practices:

- Passwords are renewed regularly, as dictated by system requirements;
- Passwords must meet length and complexity requirements, not allowing common or dictionary words;
- De-activated or expired user IDs are not granted to other individuals;
- Ekco deactivates passwords that have been inadvertently disclosed;
- Ekco monitors repeated attempts to gain access to the Services using an invalid password and takes automated actions to block repeated attempts;
- Ekco prohibits the sharing of passwords.

4. System Development and Maintenance

Ekco maintains a Secure by Design process, which includes standards and change controls procedures designed to address security requirements of the information systems, code review and testing, and security around the use of test data. Security methods include manual code review and spot checks, and penetration testing, including third party validated testing.

4.1 Change Management

The Ekco infrastructure and software change management process addresses security requirements and requires that software and infrastructure changes are documented, tested (as applicable), reviewed, and separately approved. The change management process is appropriately segregated, and all changes require approval by authorised personnel prior to any change implementation.

5. Asset Management

5.1 Physical and Virtual Asset Management

Ekco maintains a dynamic inventory of physical and virtual system assets used to perform services. System owners are responsible for maintaining and updating their service assets consistent with Ekco security standards.

Formal disposal procedures are in place to guide the secure disposal of Ekco and customer data. Ekco disposes of data when no longer required based on classification and technology assets are securely disposed of when they are no longer needed within their assigned area.

5.2 Application and System Data Management

Application and system owners are responsible for reviewing and classifying the data they store, access or transmit. Among other controls, employees and contractors are required to:

- Classify customer content as confidential information and apply appropriate access restrictions;
- Restrict the printing of customer content and dispose of printed materials in a secure manner;
- Not store corporate or confidential information on any equipment or device that does not meet the requirements of Ekco security policies and standards;
- Secure computers and data while unattended.

5.3 Data Retention

Customer content stored as part of Ekco Cloud services is accessible by the customer for a limited time period following the termination of services and then deleted (including back-up copies) in conjunction with the commercial agreement. Certain data is held for required statutory periods so as to ensure Ekco can comply with its legal obligations. Ekco has a Data Retention Policy that is compliant with the General Data Protection Regulation (GDPR).

6. Human Resources Security

Maintaining the security of customer content is one of the core requirements for all Ekco employees and contractors. Ekco's employment documentation requires all employees and contractors to adhere to Ekco policies and standards, and contain express obligations addressing the protection of confidential information as well as personal information.

All Ekco employees and contractors are subject to confidentiality obligations which are included as part of any contractual engagement with Ekco. The Ekco security team also regularly communicates to employees on topics related to information and physical security in order to maintain security awareness on specific topics.

6.1 Background Screening

Ekco currently uses background screening vendors for all new hires and requires the same for its third party supplier personnel, except where limited by local law or employment regulations.

6.2 Training

All employees are required to take induction, and thereafter annual, training on our ISO 27001 information security, data protection and GDPR policies – all designed to protect the security of both Ekco and customer confidential information.

The training covers secure operation, privacy practices, and the principles that apply to employee handling of personal information, including the need to place limitations on using, accessing, sharing and retaining personal information.

6.3 Enforcement

All employees are required to comply with all Ekco policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of employment.

7. Operations Security

7.1 Network and System Security

Ekco has ISO 27001 complaint network and system hardening standards designed to ensure that networks and systems are securely configured.

Required procedures under these standards include, but are not limited to:

- Changing or disabling default settings and/or accounts;
- Controlled use of administrative access;
- Restrict service accounts for only the purpose which they were created;
- Configure logging and alert settings appropriate for auditing.

Ekco requires the implementation of anti-malware software on servers and workstations, and regulalrly scans the network for malicious software.

Network controls govern access to customer data. These include, as applicable, (i) configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic, and (ii) network segmentation to prevent unauthorized access of customer data.

7.2 Logging

Ekco collects logs to confirm the correct functioning of our Services, to assist with troubleshooting system issues, and to protect and secure our networks. These logs may be used in monitoring the performance, stability, usage and security of the services and related components.

7.3 Protection of Data in Transit

Ekco uses secure transmission protocols for transmissionof information over public networks that are part of the services. The services are protected by encryption and access via the internet is protected by SSL connections.

8. Physical Security

8.1 Ekco office facilities

Ekco maintains the following controls designed to prevent unauthorised access to any facility:

- Facility access is limited to authorised individuals;
- Visitors are required to register and are escorted or observed at all times;
- After-hours access is strictly controlled;
- Security guards, intrusion detection, and/or CCTV cameras monitor building entry points;
- Emergency exits and evacuation routes are provided.

8.2 Data Centers

Ekco contracts with third-party data centers or cloud services for the deliveryof the services, that meet or exceed strict physical and environmental security requirements.

Ekco uses systems designed to protect against loss of data due to power supply failure including redundant service infrastructure that is set up with disaster recovery sites. Data centers and Internet service providers (ISPs) are evaluated to optimise performance regarding bandwidth, latency, and disaster recovery isolation.

Data centers are situated in facilities that are ISP carrier neutral and provide physical security, redundant power, infrastructure redundancy, and uptime agreements from key suppliers.

9. Business Continuity & Disaster Recovery

9.1 Business Continuity

Ekco strategically plans for the continuation of business operations during adverse or disruptive situations, and designs systems to keep the services operational during the occurrence of such events.

Ekco maintains emergency and contingency plans for all Ekco facilities. In the event facilities are not available, employees have the option to work remotely either at other Ekco facilities or other trusted location.

9.2 Disaster Recovery

Ekco endeavors to minimise the impact of service or operational disruptions by implementing processes and controls designed to ensure stable and orderly restoration and recovery of Ekco business systems and data. Ekco implements redundancy for all mission-critical systems, data, and infrastructure.
An ISO 27001 accreditation Disaster Recovery Plan is maintained that outlines the overall structure and approach to restoring critical systems and data, including but not limited to:

- Roles and responsibilities of individuals or teams;
- Contact information for essential personnel or third-parties;
- Recovery objectives, restoration priorities, and success metrics.

Senior management reviews and approves the plan on an annual basis, or as significant organisational changes occur.

10. Incident Response

Ekco maintains a Security Incident Response Policy that details the processes for detecting, reporting, diagnosing, and responding to Security Incidents impacting Ekco managed networks and/or systems or customer data.

"Security Incident" includes an unauthorised access to Customer data resulting in the loss of confidentiality, integrity or availability. If Ekco determines that Customer data within its control has been subject to a security incident, the affected customer will be notified within the time period required by law. Ekco's notice will describe, where known, the nature of the incident, the time period, and the potential impact to the Customer.
Ekco maintains a record of each Security Incident.

11. Vendor Management

Ekco may contract with subcontractors and suppliers to perform services. Any subcontractor or supplier shall be entitled to access Customer data only as needed to perform the specific task that they have been engaged for and shall be bound by written agreements that require them to provide at least the level of data protection and confidentiality required of Ekco. Ekco remains responsible at all times for its subcontractors' and agents' compliance with the terms of the agreement.
A list of Ekco subprocessors that may have access to Customer data can be provided on request where appropriate.

12. Compliance

Personal data is information that relates to an identified or identifiable individual. Customer determines the personal data that it includes in Customer Content. In performing the Services, Ekco acts as a Data Processor and Customer remains the Data Controller for any personal data contained in Customer Content. Ekco will act on Customer's instructions regarding the processing of such personal data, as specified in the Agreement.
Further information concerning the treatment of personal data subject to the General Data Protection Regulation, including the mechanisms employed for international transfer of such data, is provided in Ekco's Data Processing Agreement.

13. Ekco Contacts

Function	Contact
Regional Support Contact Details	https://www.ek.co/contact
Report a Suspected Security Incident	incidentteam@ek.co
Report a Suspected Data Breach	dataprotection@ek.co