Ethixbase 360 Corporate Security Practices

Classification: Internal

Table of Contents

Ethixbase 360 Information Security

As a software developer and technology provider, Ethixbase 360 takes security seriously. The Ethixbase 360 security strategy is well-defined and implemented enterprise wide.

Ethixbase 360's Information Security Program is designed to protect the confidentiality, integrity and availability of both Ethixbase 360 and customer data, such as:

- The mission and business-critical systems that customers rely upon for cloud services, technical support and other services;
- Personal and other sensitive information that Ethixbase 360 processes during its business, including customer, partner, supplier and employee data residing in Ethixbase 360's internal systems and third-party platforms; and
- Ethixbase 360 source code and other sensitive data against theft and malicious alteration.

Ethixbase 360's information security policies and practices govern the management of security for Ethixbase 360's operations, and the services provided to its customers, and which apply to all Ethixbase 360 personnel, including employees, and contractors. These policies are aligned with the ISO/IEC 27001:2022 standard and guide security within Ethixbase 360.

Ethixbase 360 has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets. Ethixbase 360 actively aligns to a variety of industry and regulatory frameworks, and best practices including the International Organisation for Standardization (ISO), System and Organisation Controls (SOC 2), National Institute of Standards and Technology (NIST), CIS v8 controls, OWASP and other industry sources.

Organisational Information Security

Ethixbase 360 has a group Chief Information Security Officer (CISO) and an IT Security Team that oversee and drive corporate information security standards, practices and controls to provide a high level of security across all critical company data and assets.

The CISO defines the policies for the management of information security across Ethixbase 360 in addition to providing the direction and advice to help protect business information assets as well as the data entrusted to Ethixbase 360 by our customers, partners and employees. The information security programs are designed to protect the confidentiality, integrity and availability of data developed, accessed, used, maintained, and hosted by Ethixbase 360.

IT Security Team

The IT Security Team are responsible for the cyber security strategy, architectural design of security solutions, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation and security technical assessment for new infrastructure.

The IT Security Team helps set internal information-security technical direction and guides all departments towards deploying information security that progress Ethixbase 360's strategic information security goals.

Ethixbase 360 Management Review Team

The Ethixbase 360 Management Review Team (MRT) oversees the implementation of Ethixbase 360-wide security programs, including security policies and data privacy standards. The MRT is chaired by the CISO.

Ethixbase 360 Product Security

The Ethixbase 360 Development and Engineering Teams are responsible for the management and improvement of the security of Ethixbase 360 products. Secure Software Development practices are embedded into the design, build, testing, and maintenance of its products throughout every phase of the product development lifecycle.

The IT Security Team works with these teams to develop, communicate, and implement secure architectures and practices, and improve the security of Ethixbase 360 products.

Compliance

Ethixbase 360's CISO and IT Security Team conduct internal audits, oversee compliance of the security controls, processes, and procedures, and proactively work with independent third parties to assess the security posture and compliance for the organisation.

Ethixbase 360 performs ongoing security evaluations as part of the company's annual compliance audits. The results of these audits are reported to the Management Review Team and Senior Leadership Team and are fed into a continuous improvement cycle that helps us keep maturing the overall security program.

Operational Security

Acceptable Use

Ethixbase 360 has formal requirements for use of the corporate network, computer systems, telephony systems, messaging technologies, internet access, enterprise data, customer data, and other company resources available to Ethixbase 360 employees, contractors and visitors.

Access Control

Access to Ethixbase 360 information systems is governed by the Access Control Policy with access to information within Ethixbase 360 granted on a least privilege and need-to-know basis. Ethixbase 360 has implemented methods and procedures designed to prevent unauthorised access to data and the systems that host that data. Appropriate authentication and authorisation methods are used to control access to network and applications including Virtual Private Network (VPN), Multi-Factor Authentication (MFA), and other supporting technical controls.

The Access Control Policy is applicable to access control decisions for all Ethixbase 360 employees and any information processing facility for which Ethixbase 360 has administrative authority.

Measures are in place to enable the timely removal of systems access rights no longer required for business purposes.

Endpoint Security

Ethixbase 360 requires the use of Endpoint Detection and Response (EDR) solutions on all endpoint devices such as laptops, desktops and servers that access sensitive data and/or infrastructure. The enterprise EDR solution is configured to perform real-time threat-definition updates and malware scans.

All computers that store or access Ethixbase 360 data must have automated security updates enabled or where appropriate security updates must be installed upon notification of their availability. All devices that process Ethixbase 360 or customer information must be encrypted using approved software.

Employees are prohibited from altering, disabling or removing endpoint security controls and the security update service from any computer. Any Ethixbase 360 employee or contractor who is identified as breaching this standard may be subject to disciplinary action up to and including termination of employment.

Monitoring

Ethixbase 360 utilises a wide range of tools to monitor its corporate and production network environments. Data is collected from devices and applications in the network and aggregated into the Security Incident and Event Management (SIEM) platform to identify, detect and respond to suspected or confirmed anomalies and threats. The SIEM is monitored by a dedicated 24/7 Security Operations Centre to respond to and mitigate threats.

Suspicious and malicious activities feed into the security-incident management process.

Security Audit Log Information

Ethixbase 360 logs certain security-related activities on operating systems, applications, databases and network devices.

Ethixbase 360 retains and reviews logs for forensic purposes and incidents. Access to security logs is provided based on need-to-know and least privilege.

Log files are protected by a variety of access controls and access is monitored.

Network Controls

Ethixbase 360 has implemented network controls for the protection and control of both Ethixbase 360 and customer data for its storage and transmission. Ethixbase 360's technical policies enforce network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems.

For administration of network security and network-management devices, Ethixbase 360 requires IT personnel to use secure protocols with authentication, authorisation and strong encryption.

Communications to and from the Ethixbase 360 corporate network must pass through cloud hosted security services which form part of the corporate network. Remote connections to the Ethixbase 360 corporate network use authorised devices and platforms). Corporate systems available outside the corporate network are protected by additional security controls such as Multi-Factor Authentication and location-based controls.

Password Management

Ethixbase 360 has implemented technical policies to enforce password requirements for the Ethixbase 360 network, operating systems, email, databases, and other accounts to reduce the risk of unauthorised access. Ethixbase 360's Password Policy is applicable to all areas of the business.

System-generated and assigned passwords are required to be changed immediately on receipt. Employees must keep their passwords confidential and always secured and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Ethixbase 360 system or applications passwords for non-Ethixbase 360 applications or systems.

Security Testing

We have a relationship with an industry-recognised penetration testing service provider to deliver security testing of both Ethixbase 360 products and the internal corporate network infrastructure.

The security testing includes internal security reviews, penetration testing, Red Team assessments and vulnerability scanning.

Vulnerability Management

Ethixbase 360 requires that appropriate security maintenance be performed against enterprise and production information systems. The company constantly works to reduce vulnerabilities in products and infrastructure, and to ensure that identified vulnerabilities are remediated as quickly as possible.

Security vulnerabilities are identified through automated scanners, internal security reviews, customer reports and external security testing. Identified vulnerabilities are tracked and assigned to the relevant system or asset owner to progress where they are subject to ongoing review until a timely resolution.

The IT Security, Engineering and Management Review Teams convene to assess track and monitor open issues and remediation progress.

Human Resources Security

Ethixbase 360 places a strong emphasis on personnel security. The company maintains ongoing initiatives intended to help minimise risks associated with human error, theft, fraud and misuse of resources, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

Ethixbase 360 maintains high standards for business conduct at every level of the company and which apply to employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Employees who fail to comply with Ethixbase 360 policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

Employee Screening

Ethixbase 360 uses an external screening agency to perform pre-employment background checks to provide assurance around the trustworthiness and reliability for newly hired

employees. Employee screening in other countries varies according to local laws, employment regulations and local Ethixbase 360 policy.

Confidentiality Agreements

Ethixbase 360 employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Ethixbase 360 obtains a written confidentiality agreement from each sub-contractor before that sub-contractor provides services.

Security Training

Ethixbase 360 employees are trained on company policies and security practices. This includes annual security training and ongoing security awareness updates. In addition, all Ethixbase 360 employees must take annual privacy training which covers privacy best practices and compliance requirements under applicable laws, including the General Data Protection Regulation (GDPR).

All new Ethixbase 360 employees attest to comply with Ethixbase 360 information security policies and attend training during the onboarding process.

Data Classification and Handling

The responsibility, inventory and ownership of Ethixbase 360's Information Assets is governed by the Data Classification and Handling Policy which provides guidelines for all Ethixbase 360 information classification and minimum handling requirements for each data type.

This policy applies to all information assets held on any Ethixbase 360 system, including both enterprise systems and cloud services.

Asset Classification and Control

Ethixbase 360 categorises information into four types – Public, Internal, Restricted, and Confidential. Each classification requires corresponding levels of security controls:

- **Public** - information is not sensitive and there is no need with it remaining confidential to Ethixbase 360.
- **Internal** - information must remain confidential to Ethixbase 360.
- **Restricted** and **Confidential** - information must remain confidential to Ethixbase 360 and access within the company must be restricted on a "need to know" basis, with additional handling requirements for Restricted and Confidential information.

Data Storage

Ethixbase 360 utilises cloud-based services provided by Microsoft Azure and Amazon Web Services (AWS) to ensure the security, scalability and reliability of our operations. All enterprise and customer data are securely stored within data centres located in UK and Ireland-based regions, ensuring compliance with data protection regulations.

Business Resilience

Ethixbase 360 maintains a formal Business Continuity Plan (BCP) that is regularly reviewed and updated. The BCP enables the company to respond quickly to most failure events, including natural disasters and system failures. The plan specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Ethixbase 360 across all areas of the business.

The goal of the program is to minimise negative impacts to Ethixbase 360 and maintain critical business processes until regular operating conditions are restored.

Incident Response

Ethixbase 360 maintains a formalised Incident Response Plan which reflect the recommended practices in security standards issued by the International Organisation for Standardisation (ISO), the United States National Institute of Standards and Technology (NIST), and other industry frameworks.

Ethixbase 360 has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.

Ethixbase 360 will evaluate and respond to any event when Ethixbase 360 suspects that Ethixbase 360-managed customer data has been improperly handled or accessed.

If Ethixbase 360 determines a confirmed security incident involving Personal Information processed by Ethixbase 360 has taken place, Ethixbase 360 will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Ethixbase 360 Services.

Information about malicious attempts or suspected incidents is Ethixbase 360 Confidential information and is not externally shared.

Risk Management

Ethixbase 360's Risk Management framework is based on the ISO 27001 Information Security Management Standard. This program takes both the company's and customer's security needs into consideration and arrives at a set of security requirements using controls listed across a range of international security standards.

The corporate Risk Register captures and tracks the risks faced by the business, their potential impact, likelihood of occurrence and the key controls and management processes to mitigate the risks.

Third Party Supplier Management

Ethixbase 360 is committed on making sure third-party supplier (including contractors and cloud service providers) engagements do not in any way jeopardise the company, our customers or their data. A review process is undertaken by the Cyber Security, Operations and Finance teams for any proposed third-party supplier engagements. For any engagements deemed high or critical risk, these are subject to additional security, compliance, and risk reviews.

Ongoing due diligence also occurs through periodic reviews - either upon contract renewal or annually depending on the risk level of the engagement.