SECURITY @ EDB

Version 1.0
Effective August 21, 2023

This Security Standard describes the security controls of EnterpriseDB's ("EDB") cloud services, software products, technical support, and consulting services delivered to customers under the relevant agreement and the applicable order. Demos, betas or preview services and internal IT systems not involved in the delivery of Services are outside of the scope of this Security Standard.

I. Security @ EDB

The EDB Security Standard describes the information security program implemented by EDB ("Information Security Program" or "Program"). The Program includes a comprehensive set of policies, procedures, and controls designed to protect the confidentiality, integrity, and availability of data and systems. The objective of the Program is to establish the ownership, accountability, and scope of EDB's information security activities. The Program aligns with applicable industry standards and best practices including but not limited to; ISO/IEC, PCI DSS, Service Organization Controls (SOC), and other regulatory bodies.

A. Oversight and Governance

EDB has an established information security department with key stakeholders who are responsible for the development, implementation, and maintenance of the Program. EDB's Chief Information Security Officer (CISO is responsible for oversight, policy strategy, compliance, and enforcement of EDB's Program.

EDB has established a formal cyber risk management program designed to identify and proactively respond to any potential threats to our products, services, or infrastructure. EDB's cyber risk program is managed by a security steering committee which consists of cross-functional management and leadership. The steering committee meets at least quarterly to provide oversight to risk management and direction in identifying, assessing, and addressing security risk.

EDB's information security policies are reviewed and updated on a regular basis. The design and operating effectiveness of EDB's policies and internal controls are continuously evaluated against the established EDB Security Control Framework. Corrective actions related to identified deficiencies are tracked to resolution.

EDB undergoes regular audits by independent third parties. The audits assess the effectiveness of EDB's security program and identify any areas that need improvement.

B. Roles and Responsibilities

EDB believes that clear roles and responsibilities are essential for the protection of its data and systems. Roles and responsibilities within the Information Security Program are as follows:

Executive Leadership

- Support the organization's Information Security Program by reinforcing the CISO's mission and executing decision-making authority to drive program goals, objectives, and priorities.
- Maintain an understanding of enterprise risks related to security.

Chief Information Security Officer (CISO)

- The CISO is responsible for information security planning and implementation.
- The CISO develops and maintains information security policies necessary to identify and successfully manage and mitigate security risks.

- The CISO manages the identification, implementation, and assessment of common security controls.
- The CISO assists senior company officials with their responsibilities for securing EDB.

CISO Staff

Support the goals of the Information Security Program as requested by the CISO.

EDB Employees

- Understand and adhere to EDB security policies.
- Implement the necessary processes and procedures to support this policy.
- Identify, report, and seek guidance from management and/or the CISO on actual or suspected deviations from this policy.

II. Program Overview

A. Asset Management

EDB maintains a comprehensive asset inventory that includes all assets, both on-premises and in the cloud. Assets are tracked and managed using unique identifiers and have designated owners. Discovery systems are in place to identify new assets as they are introduced into the environment. EDB's asset inventory is reviewed at least annually.

Formal data retention and disposal procedures are documented to guide the secure disposal and destruction of company, personnel, and customer data according to requisite compliance standards.

EDB's data center assets are protected by subservice organizations and their security practices. Security criteria are periodically evaluated and include asset management measures such as:

- Recording and authorizing the entry and exit of media at data center locations;
- Ensuring sensitive physical media is packaged securely and transported in a secure, traceable manner; and
- Prohibiting the use of portable media in datacenters unless explicitly authorized by IT or information security management.

These asset management measures help to protect EDB's data center assets from unauthorized access, use, disclosure, disruption, or destruction.

B. Identity and Access Management

EDB implements a comprehensive identity and access management policy ("IAM") that includes strong passwords, multi-factor authentication, password managers, privileged access controls, single sign-on, unique identifiers, access reviews, shared and group account restrictions, role-based logical access, remote access restrictions, conditional authorization, end-user authentication, key management, and key storage and distribution. Controls include but are not limited to:

- EDB adheres to industry standards for its password complexity, rotation, and lockout policies.
- The use of multi-factor authentication is required for all enterprise access, remote sessions and access to environments that host production systems.
- Privileged logical access to production environments is enabled through an authorized session manager; session user activity is recorded and tunneling to untrusted data environments is restricted.

- Employees, contractors, and other corporate user accounts use single sign-on (SSO) for enterprise systems.
- Access groups used in provisioning entitlements for an account are defined, with owners, and are reviewed on a regular basis. Group owners are responsible for approving access to authorized individuals.
- EDB conducts periodic access reviews by managers for the in-scope system components to ensure that access is restricted appropriately, and corrective action is taken where applicable.
- Where applicable, processes that run as part of an EDB shared hosting platform will run under unique credentials that permit access to only one customer environment.

C. Change and Configuration Management

EDB has established a process to address the lifecycle of technology change practices, including communication for maintenance and downtime. The process addresses security requirements and requires that software and infrastructure changes be authorized, formally documented, tested (as applicable), reviewed, and approved prior to deployment to product environment.

Infrastructure and software changes are managed and tracked using work management systems. The process is appropriately segregated and access to migrate or approve changes is restricted to authorized personnel.

EDB implements the following configuration management policies and processes to ensure and maintain the integrity of its systems. Secure baselines are established for key assets in accordance with industry standards. Unauthorized changes to EDB's configuration management policies are tracked and actioned in a timely manner.

D. Data Management

EDB commits to protect the confidentiality, integrity, and availability of all data entrusted to it, including EDB data and client data. EDB will implement appropriate security measures to protect data from unauthorized access, use, disclosure, disruption, or destruction. These measures include:

- Classifying data according to its sensitivity and implementing appropriate security controls for each classification level.
- The use of industry standard encryption algorithms to project confidential data at rest and in transit.
- Regularly review its encryption practices to ensure that they remain effective.
- Redacting confidential data prior to use in a non-production environment.
- Disposing of data securely in accordance with applicable laws, regulations, and contractual requirements.

EDB regularly reviews and updates its security measures to ensure that they remain effective in protecting data. EDB will also provide training to its employees on data security best practices.

E. Backup and Recovery Management

EDB maintains a comprehensive backup and recovery plan that includes daily incremental and weekly full backups of all data stores housing sensitive customer data. Backups are encrypted and securely stored in an alternate location from the source data. EDB periodically tests the backup restoration to confirm the reliability, functionality and integrity of system backups or recovery operations, at least annually.

Management approves processes and workflows and follows prescribed change management processes and approvals. Periodic testing is performed to analyze restoration processes, implementation, and data criticality analysis.

F. Business Continuity

EDB strategically plans for the continuity of business operations during adverse or disruptive situations. EDB maintains a comprehensive business continuity plan that includes a periodic business impact analysis to identify relevant threats to assets, infrastructure, and resources that support critical business functions. The business continuity plan is reviewed and approved by management and communicated to relevant team members annually. At a minimum, EDB's business continuity plan includes:

- Recovery objectives are established for critical business functions.
- Disaster recovery protocols are defined and are detailed to allow operational recovery of systems.
- Recovery scenarios are defined, including recovery point objectives (RPO) and recovery time objectives (RTO).
- Business contingency roles and responsibilities are assigned to individuals and their contact information is communicated to authorized personnel.
- Business continuity tests are performed annually.

G. Incident Response

EDB has a comprehensive incident response (“IR”) policy that includes an IR Plan, processes, training, with defined criteria for postmortems, response testing, and reporting requirements. The controls include but are not limited to:

- An IR Plan that defines the types of incidents that need to be managed, tracked, and reported, and the procedures to manage the incident through the lifecycle.
- Confirmed incidents are assigned a priority level and managed to resolve. If applicable, incident response with business contingency activities is executed.
- Incident Response Training: EDB trains First Responders annually on the best practices for evaluating an event that could become an incident and when to engage them.
- Incident Response Testing: incident response processes are tested at least on an annual basis. Results from the tests are documented and remediations prioritized.
- EDB external communication requirements are defined by type of incident, mitigations required, and possible impact to external parties including notifications.
- EDB takes its data breach notification obligations seriously and maintains a customer protection first approach, committing to an expedited notification in the event customer impact is determined.

III. Secure Operations

A. Network Operations

EDB implements a comprehensive network operations program that includes network segmentation, perimeter security, ingress and egress points, firewalls and other security controls which include but are not restricted to:

- Logical segregation of production environments based on defined and established criteria.

- Deploying Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) across critical infrastructure for continuous monitoring.
- Critical services are monitored and protected from Denial of Service (DoS) attacks.
- EDB configures its network to deny malicious network communications across the enterprise through a managed dynamic blocklist.
- EDB enables dynamic packet filtering on the network.
- Network firewall rule sets are reviewed on at least an annual basis or as required in response to major changes in the environment.
- An inventory of all ingress and egress points is established and reviewed annually.
- Network traffic for both to and from untrusted networks passes through a policy enforcement point or firewall.

B. Site Operations

Details EDB's actions for safeguarding the physical and environmental infrastructure for physical access lifecycles. It addresses the physical and environmental security requirements for accessing data center locations that are not cloud based.

EDB is committed to protecting its technology systems from unauthorized access, damage, or destruction. To help ensure the security of its systems, EDB has physical and environmental security policies in place. These policies apply to EDB corporate offices and are levied as requirements on any third-party facilities or Cloud Service Provider where EDB workloads operate. The following are some but not all of the key elements of EDB's physical and environmental security requirements:

- CSP's employ physical access control mechanisms to restrict access to authorized personnel and authorized third parties. These controls are designed to comply with all applicable regulations, including health and safety regulations, building codes, and fire prevention codes.
- Initial permission definitions, and changes to permissions, associated with physical access roles are approved by authorized personnel. Physical access that is no longer required in the event of a termination or role change is revoked.
- Access to CSP or datacenter facilities requires management approval and documented specification before being granted.
- CSP's deploy Intrusion detection and video surveillance systems at data center locations; confirmed incidents are documented and tracked to resolution.
- CSP ensures physical access points to server locations are recorded and surveillance feed is retained for 90 days, unless limited by legal or contractual obligations.
- Access records to the facility are kept at minimum 365-day retention.
- Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks. Power and telecommunication lines are protected from interference, interception, and damage.
- Uninterruptible power supply (UPS) and generators are employed to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified as required.
- Temperature and humidity levels of data center environments are monitored and maintained at appropriate levels.

C. Workplace Operations

EDB manages all enterprise devices to ensure that they are compliant with the organization's security policies. This includes but is not limited to:

- Enrolling all enterprise devices in device management.

- Maintaining an inventory of all enterprise devices and software.
- Installing endpoint security on all enterprise devices.
- Encrypting all enterprise devices.

EDB has a defined and published enterprise device baseline that outlines the requirements for managed and trusted devices. Enterprise managed devices are required for access to critical systems. Devices, applications, and software are cataloged in an inventory that is updated at a minimum annually and in accordance with appropriate security standards.

Baselines are in place and are reviewed at minimum annually or as required and include minimally:

- Devices are configured to ensure unnecessary hardware capabilities and functionalities are disabled.
- Screen lock requirements are in place.
- Users are locked out of information systems after a defined number of unsuccessful consecutive attempts.
- Accounts remain locked for a defined period or until an administrator enables the user ID.

D. Third Party Management

EDB may use vendors, third parties, and contracted resources to support its services and operations. Procurement, legal and security diligence is performed on any vendor with access to EDB's data, networks, or systems, and for any vendor providing critical product and infrastructure services. Analysis and acceptance of vendors are managed within tiers based on their criticality to the organization and its operations.

EDB enters into contractual agreements with vendors who process or store data and defines information security terms and service level agreements as part of that contractual relationship. For critical vendors, these agreements will include a Vendor Information Security Addendum that defines the responsibilities and governance requirements regarding information shared during vendor engagements.

EDB has established processes to request and review vendor provided attestation reports or vendor risk assessments to ensure the vendor maintains the standards of the agreed upon posture. For critical vendors, these reviews are performed on an annual basis. This will be requested for all critical vendors to ensure the evaluations and impact of noted exceptions of service.

EDB performs a risk assessment review to determine the data types and access that can be shared with a vendor. If material risks are identified with any vendor, EDB will attempt to mitigate the risk in accordance with internal remediation policies and strategies.

EDB maintains a list of third-party vendors and approved relationships. This list is reviewed, and updated on a periodic basis. All EDB vendors who hold critical data and who have network access are proactively reviewed and continuously monitored.

E. Vulnerability Management

EDB has an established framework for reviewing, evaluating, and verifying malware protection, conducting penetration testing and production scanning of the environment and infrastructure. This includes the remediation timelines for triaged vulnerabilities.

EDB monitors applications, systems, and its environments for vulnerabilities on a regular cadence with automated vulnerability scanners. Additionally, EDB has an established penetration testing function which periodically conducts tailored pen-tests against production environments.

Any identified findings or vulnerabilities are required to be remediated on a timeline which is determined by a vulnerability's severity level. Remediation timelines align to industry standards and best practices which are defined as follows:

- Critical Severity - triaged within 72 hours and addressed within 14 days.
- High Severity - addressed within 30 days.
- Medium Severity - addressed within 90 days.
- Low Severity - addressed within 150 days or best effort unless tied to risk mitigation.

In case that a patch, update, or permanent mitigation is not available, appropriate countermeasures will be used to reduce the risk of exploitation of the vulnerability. This process is formally documented via a vulnerability deferral program which is used to track deferrals into future remediation.

- Secure configuration baselines are in place and are reviewed on an annual basis, or as needed.

IV. System Lifecycle and Monitoring

A. System Lifecycle

EDB is committed to protecting its technology systems from unauthorized access, damage, or destruction. To help ensure the security of its systems, EDB has made commitments to manage capacity, firmware, patch, and release management practices.

EDB follows a formal systems lifecycle methodology to govern the development, acquisition, implementation of changes, and maintenance of information systems, software, and related technology requirements. This includes adequately transitioning End of Life (EoL) and/or End of Support (EoS) software, systems, or technologies.

EDB has an established Application Security program to define security controls and processes to be used by developers within the organization. This includes managing source code with approved version control mechanisms, and ensuring code deployments are reviewed and approved by an authorized manager or designated process owner. As part of the development pipeline, EDB checks source code for vulnerabilities, including code injection, buffer overflows, insecure cryptographic storage, insecure communication, improper error handling, high-risk vulnerabilities, cross-site scripting, improper access control, cross-site request forgery, and broken authentication session management.

EDB manages and installs security-relevant patches for operating systems in accordance with priority which is determined by a finding's severity level. Patch management timelines align to industry standards and best practices, and absent exceptional circumstances, EDB operates under the following resolution timelines:

- Critical Severity - triaged within 72 hours and addressed within 14 days.
- High Severity - addressed within 30 days.
- Medium Severity - addressed within 90 days.
- Low Severity - addressed within 150 days or best effort unless tied to risk mitigation.

B. System Monitoring

EDB collects and uses logs for providing, securing, managing, measuring, and improving its ability to troubleshoot system issues, identify security events, and to protect and secure its networks and products. Logs may also be collected for compliance with agreements, policies, applicable law, or regulatory requirements. Logging may include monitoring the performance, stability, usage and security of services and related components along with defined critical information system activity.

EDB defines security monitoring alert criteria that includes but is not limited to the following parameters:

- Monitoring all individual user access with root or administrative privileges.
- Invalid logical access attempts.
- Limit viewing of logs by authorized personnel.
- Monitoring of activities based on system log in.
- Individual authorized user access attempts.
- Reports on audit logs ‘cleared.’

An established process exists for flagging alerts, and for sending confirmed alerts to authorized personnel for triage and response.

V. Training and Insider Threat

EDB requires all new hires and contractors to pass a background check as a condition of employment. Candidates are interviewed to assess, among other things, insider threat risk. All new EDB personnel go through HR and IT onboarding, which includes a requirement to assent to all key company policies.

In addition, EDB has established training and awareness program to ensure that all EDB personnel, contractors and clients who use EDB systems and data are aware of their responsibility to safeguard EDB internal and confidential data.

- All EDB personnel and contractors must complete a Security Awareness training at onboarding and at minimum refresh their training annually. Training includes EDB policies, and how to report security events to the authorized response team.
- Personnel with key security responsibilities complete relevant role-based training on an annual basis.
- EDB’s software engineers are required to complete training based on their role. Training content varies between industry relevant secure coding techniques and best practices.