HCL IntelliOps
Event Management

HCLSoftware

# Security Trust Center Document

# Table of Contents


1 **Our Commitment to Security & Trust** ........ 6

2 **Introduction** ........ 7

3 **HCL IEM** ........ 8

3.1 Security ........ 9

3.1.1 Secure by Design ........ 9

3.1.2 Secure Product Development ........ 10

3.1.3 Secure distribution of binary ........ 11

3.1.4 Compliance and Certifications ........ 11

3.1.5 Human Resources Security ........ 11

3.1.6 Infrastructure and Physical Security ........ 11

3.2 Risk management ........ 12

3.2.1 Responsibility for Risk Management ........ 12

3.2.2 AI Risk Management ........ 13

3.3 Responsible AI ........ 13

3.3.1 Secure MLOps Lifecycle Management ........ 15

4 **Data Privacy** ........ 19

4.1.1 PII Data ........ 19

4.1.2 Storage Backup and Restore ........ 20

4.1.3 Disaster Recovery ........ 20

5 **Summary** ........ 21

# Table of Figures

Figure 1 - Secure Product Development ..................... 10

## Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this Guide.

| Version Date | Description |
|---|---|
| December, 2025 | HCL_IEM _v1.3_Security_Trust_Center_Document |
| July, 2026 | HCL_IEM _v1.4_Security_Trust_Center_Document |

# 1 Our Commitment to Security & Trust

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundations of our products. The HCLSoftware security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

# 2 Introduction

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundations of our products.

The HCLSoftware security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

This Trust Center document provides a transparent overview of the principles and practices governing HCL IntelliOps event management (HCL IEM), giving you the confidence to leverage the AI-powered real-time event intelligence platform to manage your hybrid-cloud environments.

# 3 HCL IEM

HCL IntelliOps Event Management (IEM) is an AI-driven platform for IT event management and automation, equipping organizations with advanced capabilities. It delivers real-time, topology-aware alert correlation, ML-powered pattern detection and intelligent remediation.

The product offers seamless integration with an organization's existing element monitoring tools. This is achieved using the Integration Management Module (IMM), a component of HCL IntelliOps Event Management that offers single-click connectors for seamless integration with leading element monitoring solutions. With AI-driven capabilities, HCL IntelliOps Event Management identifies root causes, predicts outages, and reduces mean time to resolution, fostering collaborative teamwork and delivering real-time actionable insights.

This streamlined approach enhances cost savings, system resilience, and the end-user experience, making it an invaluable asset for optimizing IT operations on a global scale.

IEM applies AI/ML techniques for dynamic event correlation, and metric-based anomaly detection. Its Generative AI capabilities are delivered through a native Gen AI add-on component, which brokers enterprise foundation models and enforces model governance.

- **ML capabilities in IEM:**
  - **Dynamic/ML-based correlation**: IEM's AI algorithm learns patterns from historical alert data, with a feedback system to refine grouping accuracy over time and avoid pulling irrelevant alerts into an actionable.
  - **Metric-Based Anomaly Detection:** Continuously analyzes metric patterns (e.g., URL response time, DB latency, CPU usage) using ML-based or static threshold models to detect anomalies and predict potential issues, reducing false positives.
  - **Runbook Recommendation and prediction:** This feature analyzes individual tickets, compares them against 4000 runbooks and 500 fixlets, and recommends best automation for resolution along with a confidence score.
  - **GenAI features offered by HCL IEM:** IEM's GenAI engine leverages Azure OpenAI's GPT model to provide following features:
    - **Alert Insight and Analysis:** Lets users query alerts and actionable in natural language; the GenAI engine summarizes issues, surfaces probable root causes, and presents key contextual data tied to the actionable
    - **Integration with Automation Libraries and Change Management:** Analyzes alerts alongside change, problem, and automation data from integrated sources like ITSM platforms (ServiceNow, HCL BigFix Service Management), and runbook/automation libraries (Ansible Tower/AWX, HCL BigFix), matching each alert with related change tickets to help users understand frequency and possible root cause.
    - **Workflow-Driven Automated Remediation:** Diagnoses actionable alerts and correlates them with change tickets and available automation runbooks, letting users trigger pre-approved automation directly from the workflow with a human-in-the-loop approach for reliability and security.

## 3.1 Security

We integrate security into every phase of the product lifecycle, from concept to deployment, to protect your data and infrastructure.

### 3.1.1 Secure by Design

HCL IntelliOps Event Management (HCL IEM) SaaS on GCP is developed in-house following a secure software development lifecycle. The product undergoes a comprehensive threat modelling assessment to proactively identify, evaluate, and mitigate potential security risks from the ground up.

- **Authentication and Authorization**:
  - **Single Sign-On (SSO)**: User authentication is managed via SSO, integrating with enterprise Identity Providers (Azure AD, Okta) over SAML 2.0.
  - **Role-Based Access Control (RBAC)**: A fine-grained RBAC model is enforced to ensure users and services have access only to the resources necessary for their roles.
  - **API Security**: All API endpoints require authentication, using JWT token.
  - **Session Management**: Idle user sessions are automatically terminated after 60 minutes of inactivity to mitigate the risk of unauthorized access from unattended sessions.
- **Secure-by-Design Architecture**: Adheres to best practices for data encryption, access controls, and secure authentication mechanisms.
  - **Data encryption at rest** – In HCL IEM's IMM confidential data (User secrets) are encrypted at rest using the AES GCM encryption. Additionally, for IEM SaaS, confidential data is stored in GCP Secret Manager and are encrypted at rest using Cloud native features.
  - **Data encryption in transit** – All access to your instance over the internet is encrypted using Transport Layer Security (TLS) with TLS1.2 and above version cipher suites. All HTTP requests are automatically redirected to HTTPS. We also recommend using encryptions for all integrations.
  - Following are the security control for Gen-AI Add on component in IBM Cloud:

    Key features include:
    - TLS 1.2 and 1.3 encryption for data in transit and AES-256 encryption for data at rest.
    - Encrypted data at rest and in transit.
    - Strict role-based access controls (RBAC).
    - Integration with Cloudflare DNS and Global Load Balancer, which also brings in layer 7 firewall capabilities, including WAF and DDoS protection for secure routing.
    - Controlled agent execution through tool authorization, runtime safeguards, and
    - monitored operational controls.
    - Execution traceability and auditability to support operational monitoring, governance review, and investigation of agent activity.
    - Secure secrets handling through approved platform mechanisms, so credentials are not exposed in prompts or knowledge assets.

### 3.1.2 Secure Product Development

HCLSoftware adheres to stringent development processes to produce the code and provide to our customers. All Development practices incorporate change control and are the key criteria assessed at release approval stage including key practices around following

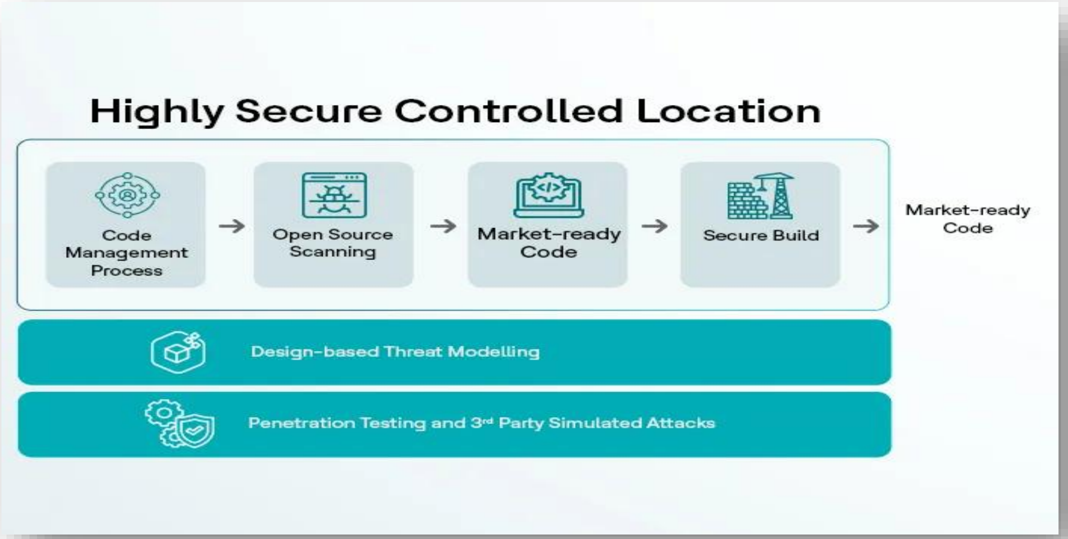


Figure 1 - Secure Product Development

1. **Requirements & Planning**
   - **Data Privacy Assessment**: HCL's Privacy and Data Protection by Design and Default (PbD) addresses privacy requirements during design and verification phases. HCL Software uses the One Trust Platform to perform Data Privacy assessments for products, platforms, and operations support.
2. **Design**
   - **Threat Modelling**: The process of identifying and prioritizing potential threats to a system and finding mitigation strategies.
   - **Secure Design Review:** Secure Design Review is an assessment done for a product by the HCLSoftware Security team to understand the product architecture, means of deployment / delivery and various other security measures which are in place, as per the industry standards
3. **Development**
   - IDE-Level Code Linting
   - Open-Source Code Composition and Vulnerability Analysis
   - Static and Dynamic Application security testing
   - Penetration Testing - Internal penetration testing is done for every release, and external testing is conducted annually.
4. **Maintenance**
   - **Security Bulletins & Vulnerability Management**: The HCL Product Security Incident Response Team (PSIRT) manages the receipt, investigation, and internal coordination of reported security vulnerabilities for HCL Software product offerings. The PSIRT coordinates with product

development teams who investigate reported vulnerabilities and identify the appropriate response plan. For more information, visit the [HCLSoftware PSIRT page](#).

- The HCL PSIRT publishes Security Bulletins describing any relevant CVEs and pointing to additional details and remediation. A list of security bulletins for HCL IntelliOps event management (HCL IEM), can be found on the official HCL Software support and community forums.
- **Product Security Training**: Periodical training sessions are conducted for product teams on Secure Development, ISMS, Data Privacy, PSIRT Process, and more.

#### 3.1.3 Secure distribution of binary

The binaries for the product are securely distributed via MHS Portal. My HCLSoftware (MHS) is a web application for HCLSoftware customers and partners that provides a new and improved way to find and quickly download the latest HCLSoftware product releases as well as supported older releases. All binaries are cryptographically signed. MHS provides seamless access to resources and tools designed to effectively manage the use of HCLSoftware products and services.

#### 3.1.4 Compliance and Certifications

The HCL IntelliOps event management (HCL IEM), platform has the following compliance certification/attestation available:

- ISO 27001
- SOC 2 Type II
- SOC 3
- ISO 27034

#### 3.1.5 Human Resources Security

Human resources security practices, background checks, and training processes are taken care of by the HCL Software team.

#### 3.1.6 Infrastructure and Physical Security

IEM leverages the robust physical and environmental security controls of its cloud partner, Google Cloud, Network and Perimeter Security

– The IEM network is designed to protect against external threats and ensure secure communication.
  - **DDoS Mitigation & perimeter Defence**: We utilize GCP Cloud Armor and Firewall as a protective layer at the network edge to protect against both volumetric and application-layer Distributed Denial-of-Service attacks, ensuring service availability.
  - **Network Isolation**: All application and data services communicate over a secure, private internal network within the GCP Cloud environment. This isolates critical components from the public internet, reducing the attack surface.

- **Secure Transport**: All data in transit, both externally and internally between microservices, is encrypted using Transport Layer Security (TLS) 1.2 or higher with industry-approved cipher suites. All HTTP traffic is strictly redirected to HTTPS.
- **Cloud Provider Data Security**: GCP Cloud manages infrastructure-level data security, compliance, and physical safeguards. More details can be found in GCP Cloud's Data Security Overview.
- **24 * 7 Security Monitoring**: The Entire platform is under observation with a Security Information and Event Management (SIEM) using Exabeam solution managed by HCL SW.

– The HCL IEM Gen AI Add-On (hosted on IBM Cloud) leverages the robust physical and environmental security controls of its cloud partners, including IBM Cloud for Application hosting and Microsoft Azure for LLM models.

- **Network and Perimeter Security**: The HCL IEM Gen AI Add-On network is designed to protect against external threats and ensure secure communication.
- **Perimeter Defence**: We utilize Cloudflare as a protective layer at the network edge. This provides:
  - **Web Application Firewall (WAF):** To detect and block common web attacks like SQL injection and Cross-Site Scripting (XSS).
  - **DDoS Mitigation:** To protect against both volumetric and application-layer Distributed Denial-of-Service attacks, ensuring service availability.
- **Network Isolation:** All application and data services communicate over a secure, private internal network within the IBM Cloud environment.
- This isolates critical components from the public internet, reducing the attack surface.
- **Secure Transport:** All data in transit, both externally and internally between microservices, is encrypted using Transport Layer Security (TLS) 1.2 or higher with industry-approved cipher suites. All HTTP traffic is strictly redirected to HTTPS.
- **Cloud Provider Data Security:** IBM Cloud manages infrastructure-level data security, compliance, and physical safeguards. More details can be found in IBM Cloud's Data Security Overview.
- **Monitoring**: The Entire platform is under 24*7 observation with a Security Information and Event Management (SIEM) maintained by HCL SW.

## 3.2 Risk management

HCL Software has a formalized risk management program that aligns with ISO 31000 and ISO 27005 best practices, as well as ISO 27001/27002.

Risk management processes are integrated with other management systems, such as the Information Security Management System (ISMS). Security controls are implemented in accordance with our ISMS to manage risk across the organization.

### 3.2.1 Responsibility for Risk Management

To drive the remediation of risks, our program reports risk status and escalates where necessary to senior management to inform business decision-making. Senior executives have overall responsibility as risk owners for mitigation, avoidance, transference, or acceptance of the risk.

HCL Software uses a combination of weekly, monthly, and quarterly meetings and reports to ensure communication of risks.

Every HCL Software staff member is responsible for the effective management of risk, including the identification of potential risks, the development of risk mitigation plans, and the implementation of risk reduction strategies.

#### 3.2.2 AI Risk Management

HCLSoftware has defined processes and procedures for managing and accessing information systems and operational security risks. HCL IntelliOps event management (HCL IEM) undergoes regular assessments to identify and assess the likelihood and impact of risks.

These potential risks include unauthorized access, use, disclosure, or disruption to HCL IntelliOps event management (HCL IEM), systems and customers. Risks are categorized in accordance with a formally documented procedure.

Any identified risk is managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of HCL IntelliOps event management (HCL IEM), systems and customer data.

### 3.3 Responsible AI

At HCLSoftware, we are committed to developing and deploying Artificial Intelligence in a manner that is ethical, transparent, and trustworthy. Responsible AI is a core principle that guides the design, implementation, and ongoing improvement of AI-powered capabilities in HCL IntelliOps Event Management (IEM).

The Gen AI Add-on for HCL IEM integrates AI responsibly to enhance automation, improve workflows, and deliver experiences. HCL Software promotes safe, transparent, and ethical AI usage.

| Control | Description |
|---|---|
| Content Filtering & Prompt Validation<br>(using Azure native content filtering service) | • Real-Time Content Filtering: Built-in content moderation checks for toxic, harmful, or restricted content using classifiers and guardrails before generating output.<br>• Prompt Injection Protection: Input sanitization and pattern recognition techniques are used to detect and neutralize prompt injection attempts.<br>• Output Filtering: Sensitive terms, data leakage, or prohibited topics are blocked before reaching the user.<br>• Runtime Safeguards: Input and output safeguards help enforce scope, confidentiality, and safe response behavior during agent execution. |

| | |
|---|---|
| Responsible AI – Risk & Incident Management | • Conducts an AI Risk Assessment for every major release.<br>• Maintains structured processes for identifying, reporting, and resolving AI-related security incidents. |
| Responsible AI – PII Protection | Follows a "purposeful, limited, and minimized" approach for handling PII.<br>• Uses regex-based sanitization to redact sensitive data and prevent exposure.<br>• Processes only the minimal data required for operational needs.<br>• Allows display of a customizable banner to notify users not to provide or prompt any sensitive/PII data when interacting with AI agents. |
| Responsible AI – Accuracy & Transparency | • Supports tuning of AI hyperparameters to improve accuracy and groundedness.<br>• Promotes transparency and clarity in AI-driven workflows.<br>• Provides visibility into agent execution flow, including conversation steps, tool calls, and outcomes. |

We take a defense-in-depth approach to securing Generative AI systems, covering user data, model interactions, infrastructure, and ethical governance.

1. **User Data Protection**
   - **Encryption in Transit and at Rest**: All user inputs, outputs, and metadata are encrypted using TLS 1.2/1.3 for data in transit and AES-256 for data at rest.
   - **Zero Retention of Sensitive Inputs**: User prompts or responses classified as sensitive are not retained unless explicitly required and approved by the customer.
2. **Access Control & Identity**
   - **Role-Based Access Control (RBAC)**: Fine-grained access is enforced to ensure only authorized users can interact with or configure AI services.
   - **Single Sign-On (SSO) & SAML 2.0 Integration**: Federated identity ensures authenticated access aligned with enterprise identity providers.
   - **Audit Logs**: All access and activity logs are captured and monitored for suspicious behaviour.
3. **API & Model Access Security**
   - **API Key Management**: API keys are securely generated, rotated, and stored in encrypted vaults (e.g., GCP Secret Manager).
   - **Scoped Access**: APIs are protected with least-privilege permissions and rate-limiting to avoid abuse or overuse.
4. **Content Filtering & Prompt Validation**

- **Real-Time Content Filtering**: Built-in content moderation checks for toxic, harmful, or restricted content using classifiers and guardrails before generating output.
- **Prompt Injection Protection**: Input sanitization and pattern recognition techniques are used to detect and neutralize prompt injection attempts.
- **Output Filtering**: Sensitive terms, data leakage, or prohibited topics are blocked before reaching the user.
- **Runtime Safeguards:** Input and output safeguards help enforce scope, confidentiality, and safe response behaviour during agent execution.

5. **Secure Development Practices**
    - **OWASP for GenAI**: Regular testing is conducted against OWASP Top 10 for Large Language Models (LLMs), including:
        - Prompt injection
        - Model denial-of-service (DoS)
        - Insecure plugin design
        - Sensitive information disclosure
        - Inadequate sandboxing
        - Supply chain vulnerabilities
    - **Defender for Cloud**: Continuous security posture management with Azure Defender for Cloud (or similar services) ensures compliance, threat detection, and remediation for AI workloads.
6. **Responsible AI and Ethical Safeguards**
    - **Explainability & Auditability**: All AI outputs are traceable with logs and rationales for key decision-making.
    - **Human-in-the-Loop Review**: Critical actions or high-risk decisions include human validation checkpoints.
    - **Transparent Use Notification**: Users are informed when they're interacting with AI systems, maintaining ethical transparency.
    - **Operational Governance:** Guardrails, controlled execution, and agent disablement procedures help support safe and governed production use of AI agents.

### 3.3.1 Secure MLOps Lifecycle Management

HCL IEM delivers its AI/ML capabilities through the AIML Toolkit, a containerized microservice that manages the end-to-end machine-learning lifecycle: data sourcing, preparation, model training, validation, deployment, inference, and drift-based retraining.

Security is embedded at each stage of this MLOps pipeline, and the controls described below operate in addition to the platform-wide protections covered earlier in this document:

- Model Training and Customer Data Segregation
    - Customer-specific training data: Models are trained on the data of the individual customer (tenant) for whom the objective is defined. Training data is sourced at job runtime from that customer's

own databases or object-storage location. Datasets are not pooled or shared across customers, and one customer's data is never used to train another customer's models.

- Per-customer and per-environment models: Every customer environment maintains its own models. Model artifacts, evaluation metrics, and job status are stored in a dedicated per-customer object-storage bucket and versioned by objective name, objective version, and algorithm code. This provides per-customer, per-objective, per-version, and per-algorithm isolation and supports independent promotion across environments.
- Logical and physical segregation: Logical segregation is enforced through dedicated per-customer storage and databases, fine-grained RBAC, and scoped service credentials retrieved from the secret manager. Physical and infrastructure segregation, together with encryption at rest, is provided by the underlying Google Cloud platform. Training, testing, and inference for a given customer execute only within that customer's data boundary.

1. **Training Data Security**
   - Secure ingestion: Training data is ingested at runtime from the customer's approved sources (MySQL / ClickHouse databases or GCP object storage) over the platform's private internal network. Database credentials are never embedded in the application; they are retrieved on demand from Google Cloud Secret Manager using the service's managed workload identity and are resolved per job.
   - Secure storage: Training datasets, drift baselines, and model artifacts reside in per-customer GCP object storage and databases. Data in transit is protected using TLS 1.2 or higher.
   - Secure processing: Data is streamed and processed in bounded batches to avoid unbounded scans and memory exhaustion. During preparation, free-text fields are normalized and sensitive tokens - such as email addresses, IP addresses, and file paths - are automatically masked before feature engineering, reducing exposure of sensitive content in derived features and logs.
2. Access control, monitoring, and auditing: Access to data and models is governed by least-privilege RBAC and scoped credentials.
3. **Protection Against Data Poisoning and Model Attacks**
   - Pre-training data validation and quality checks: Before a dataset is used, it passes through validation and preparation - schema and feature selection, handling of null and invalid values, data-type inference and coercion, and text normalization/sanitization. Empty or malformed datasets cause the job to fail safely, and outliers are handled through required transformations for robust model fitting.
   - Anomaly and drift-based gating: Newly observed data is continuously compared against an established baseline using statistical tests to detect distribution shifts, which also helps surface anomalous or manipulated data before it is adopted into a retrained model. Retraining is recommended only when a material share of features drift.
   - Model integrity and anti-tampering: Model artifacts are stored in access-controlled, per-customer object storage with least-privilege credentials, protecting them from unauthorized access or modification.

- Model theft and abuse protection: Inference and management APIs require authentication and are protected by RBAC, least-privilege scoping, and rate limiting at the platform gateway, mitigating model-extraction and abuse risks.
- Adversarial testing scope: IEM's models are statistical/classical ML models that operate on the customer's own operational event data rather than on externally exposed generative models, so classical adversarial example attack surfaces are limited.

4. **Model Security Controls**
   - Secure development practices: The MLOps pipeline is built and released under HCLSoftware's secure SDLC - threat modeling, secure design review, open-source composition and vulnerability analysis, static and dynamic application security testing (SAST/DAST), and penetration testing - as detailed in Secure Product Development.
   - Hardened runtime: The toolkit is packaged as a minimal, hardened container image that runs as a non-root user with read-only application layers and no interactive shell in the runtime image; generated model files are written only to isolated scratch space.
   - Model validation and approval gates: During AutoML training, multiple candidate models are trained and compared before selection. Objective, version, and algorithm governance is handled in the IEM platform, and training and retraining jobs can be initiated only by authorized, RBAC-controlled roles, with the requester recorded.
   - Model registry and versioning: Trained models are kept in a controlled, per-customer object-storage registry, versioned by objective, version, and algorithm, alongside their evaluation metrics and job-status metadata. Access is restricted through RBAC and scoped credentials.
   - Deployment and monitoring controls: Deployments are containerized on minimal hardened base images with runtime security constraints (non-root, read-only filesystem, and health checks). Runtime behavior is monitored through Google Cloud Logging and the platform SIEM under 24x7 security monitoring.
5. **Testing and Validation Parameters**
   - Security testing: Security testing during development and release follows the secure SDLC - SAST, DAST, software composition analysis of open-source and third-party components, internal penetration testing for every release, and annual external penetration testing - coordinated with the HCL Product Security Incident Response Team (PSIRT).
   - Model performance validation: Model quality is validated during training. For classification objectives, multiple candidate algorithms are trained and compared, and performance metrics (for example, Accuracy, AUC, and F1-score) are computed and persisted per objective and algorithm; forecasting and regression objectives use appropriate error and goodness-of-fit measures.
   - Drift monitoring parameters: Drift is measured using the Kolmogorov-Smirnov test (numerical features) and the Chi-Square test (categorical features), the Cramer's V effect size, and a per-feature drift ratio determines whether retraining is recommended.
   - Robustness and bias considerations: Robustness is addressed through data-quality validation, outlier handling, and continuous drift monitoring. Because IEM's models operate on operational IT

event and telemetry data and generally do not process protected personal attributes, demographic bias/fairness testing is typically not applicable; where relevant, continuous evaluation together with model-specific explainers and model cards is used to monitor for accuracy degradation and unintended outcomes.

- Pre-production security assessment: Prior to production deployment, changes undergo secure design review, the SAST/DAST/SCA and penetration-testing gates noted above, container image hardening and vulnerability checks, and third-party and GenAI component vetting. The platform maintains ISO 27001 and SOC 2 Type II attestations.

# 4 Data Privacy

Data privacy (also called information privacy) refers to the right of individuals to control how their personal information is collected, used, shared, and stored. It's about ensuring that personal or sensitive data is handled in ways that protect people's rights and maintain their trust.

Data privacy for the HCL IntelliOps event management (HCL IEM) Platform refers to the protection of customer data by implementing strong technical and organizational controls.

The platform is designed to secure customer-owned data through encryption, strict access controls, and secure cloud infrastructure.

- Data Roles and Responsibilities:
  - In our relationship, the customer is the data controller, retaining full ownership and control over the data collected and determining the purpose of its use. HCL Software acts as the data processor, processing data only on behalf of the controller and in accordance with our contractual agreement. For more information visit [HCL Software Privacy]
- Purpose Limitation and Data Minimization:
  - The platform is designed to process personal data for the sole purpose of product administration and fulfilling our contractual obligations. We practice data minimization, and the product is not designed to process any special categories of sensitive personal data.
- Customer Information Processed:
  - The platform may process the following customer information as part of its standard functionality:
    - **Contact Information:** Organizational Email Address
    - **Personal Identification:** First Name, Full Name, Last Name
    - **User Account Information:** Login ID
  - Additional fields for Gen AI Add on Component:
    - Browsing Information - Session Time and IP Address
    - Business Unit name/Company/Customer Name
    - Conversation chat data

### 4.1.1 PII Data

In HCL IEM, we collect the following types of information from Customers, and the overall purpose of the data is to provide operations Support and to improve the end user experience for that particular customer.

a. **First Name/Last Name/Full Name**: We collect information about the end user from the Customer for First Name/Last Name and Full Name for general maintenance, support, and to improve the Support Services for the customer. Data is collected via integration with Customer SSO.
b. **Organizational Email Address/Login ID** – We collect information about the end user from the Customer for Organizational Email Address and Login ID for general maintenance, support, and to improve the Support Services for the customer. Data is collected via integration with Customer SSO.
c. **Conversation chat data** – The chat data from the user comprises mostly the user query, where the user can type their query as part of the Chatbot interface, and the text will be stored in an encrypted manner.
d. **Browsing Information** – Session Time and IP Address – We collect information of the end user from the Customer for Session Time and IP Address via the Request Header of the

payload (for the conversation interaction between user and HCL IEM Gen-AI Add-on). The purpose of this data is to provide support and improve the support services in the case of issues like Latency, connectivity issues, or end-user experience improvement.

### 4.1.2 Storage Backup and Restore

As part of the base Service, HCL provides storage snapshot backups for data protection of file systems. Storage snapshot backups include supporting data availability, configuring snapshot and replication schedules, and facilitating restore of data from snapshots. Application logs are retained for up to 30 days and access logs are retained up to 1 year. Additional backup and restore capacity and services are available upon request and for an additional charge.

### 4.1.3 Disaster Recovery

In the event of an HCL declared Disaster, HCL will communicate with Customer as to the status of the recovery process, including progress regarding the Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO"). The defined RPO/RTO duration is 8 hours RPO, 8 hours RTO.

- HCL provides the ability to failover a full copy of Customer data to a designated standby environment at a geographically disperse DR location within the defined RPO and RTO. HCL manages storage disaster recovery utilizing a replication of storage snapshots to achieve the required RPO/RTO.
- Storage snapshots provide a point-in-time capture of Customer data using the HCL managed storage infrastructure. Differential data changes between snapshots are replicated to offsite storage for maintaining synchronization of the Customer data. Snapshot and replication frequency is determined by the defined RPO/RTO. Storage capacity is allocated per Gigabyte as necessary to meet the Customer contracted disaster recovery requirements.

For the HCL IEM Gen-AI Add-on following are the data retention policies on IBM Cloud

**Data Retention (for HCL IEM Gen-AI Add-on hosted on IBM Cloud)**

- As part of HCL IEM Gen-AI Add-on, all data that is being captured or processed has a retention period after which the data will be scraped or purged securely.
- The default retention period involves archival after 1 year or a period in compliance
- with customer security policy.
- Post 1 year, the data will be archived for 3 months, which can be restored in case requested by customers. The data retention period can be customized as per the customer's requirement.

## 5 Summary

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure AI-powered real-time event intelligence platforms to our customers. For more information, please contact us

HCLSoftware

hcl-software.com