HCLSoftware

HCL BigFix Service Management

Security Trust Center Document

Version 1.0

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Table of Contents

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
September, 2025	HCL BigFix Service Management Security Trust Center v1.0

1 Introduction

This document outlines the foundational principles, security controls, and governance frameworks that ensure the confidentiality, integrity, and availability of customer data across our Software as a Service (SaaS) offering. This document serves as an overview of how HCL BigFix Service Management safeguards enterprise data, supports compliance with global standards, and integrates responsible AI practices into its platform.

Our approach is rooted in industry-recognized security principles such as Defense-in-Depth, Secure-by-Design, and Zero Trust, and is operationalized through a robust Governance, Risk, and Compliance (GRC) program. Whether it's infrastructure security, access control, data encryption, or AI governance, each layer of our service is designed to meet the evolving needs of modern enterprises while maintaining trust and accountability.

This document is intended for customers, partners, and stakeholders who seek clarity on how HCL BigFix Service Management protects data, ensures operational resilience, and complies with regulatory obligations in a multi-tenant SaaS environment

2 Scope of Document

HCL BigFix Service Management supports two deployment models:

- Software as a Service (SaaS)
- On-Premise Deployment

In the On-Premise model, the customer is responsible for provisioning and managing all underlying infrastructure, including security controls, data encryption, backup, and retention policies. As such, this document exclusively addresses the SaaS deployment of HCL BigFix Service Management. The guidance and controls outlined herein may not apply to On-Premise implementations.

3 Core Security Principles

The deployment of HCL BigFix Service Management (SaaS) and associated AI components adheres to three industry standard principles.

3.1 Defence-in-Depth

This is a layered approach to security. This principle assumes that no single security control is infallible. Therefore, the platform is protected by multiple, redundant, and overlapping security measures across its entire technology stack.

- Multiple layers of protection
- Redundant mechanisms to prevent, detect, and respond to threats

3.2 Secure-by-Design

The secure-by-design principle dictates that security considerations are integrated into the entire product lifecycle, from the earliest stages of conception and design through development, testing, deployment, and maintenance.

- Threat modelling during design phases
- Static and dynamic application security testing (SAST/DAST) during development
- Independent and rigorous penetration testing before release

3.3 Zero Trust

In a Zero Trust architecture, no user, device, or application is trusted by default, regardless of whether it is inside or outside the corporate network.

All access requests require strong authentication via Federated Authentication or SSO, fine-grained authorization with RBAC, and encryption in transit with TLS 1.1+ for all external communications.

4 Data Security and Protection

Data security is a foundational aspect of our AI implementation strategy. Regardless of the underlying infrastructure or technology stack, we follow industry best practices to ensure that data processed by AI systems is protected against unauthorized access, misuse, and breaches

4.1 Customer Responsibility

While HCL BigFix Service Management enforces strong confidentiality controls, customers are encouraged to classify their data appropriately and configure access policies within their instance to align with their internal governance requirements.

4.2 Infrastructure Security

Our data storage and processing environments are hosted on secure, enterprise-grade infrastructure providers that implement stringent physical and network security controls. These include identity and access management, data centre surveillance, and hardened server configurations.

4.3 Access Control

Access control is a critical security measure that protects customer data from unauthorized access. By default, access to the HCL BigFix Service Management instance is secured using password-based authentication, and users are granted role-based access to product features, following the principle of least privilege.

4.4 Authentication

User accounts can be provisioned either manually via the administration console or automatically through integration with an external identity store such as LDAP or integrating with an IdP that supports SCIM. It is recommended to populate only the user attributes essential for service functionality. For instances using native authentication, passwords are securely stored within the application infrastructure. To ensure password security, the following best practices are recommended to be implemented by users of HCL BigFix Service Management:

- Passwords should be at least twelve (12) characters long
- Password should be a combination of any three of the below:
  - At least one character in uppercase alphabets (A-Z)
  - At least one character in lowercase alphabets (a-z)
  - At least one numeric character (0-9)
  - At least one special character [$,!,#,%,*, &,(,),@]
- Passwords must not be shared between users or exposed on public platforms.
- If a password is suspected to be compromised, it must be changed immediately.

For enhanced security and user experience, it is strongly recommended to integrate the instance with a SAML 2.0-compliant Identity Provider (IdP) such as Entra ID, Okta, or Ping Identity. This integration allows

customers to enforce their own password policies and enables Single Sign-On (SSO). Additionally, Multi-Factor Authentication (MFA) can be configured through the IdP to further strengthen access controls.

4.5 Authorization

Upon successful authentication, users are granted access to product features based on their assigned roles. Roles can be assigned directly to users or to user groups via the administration console.

HCL Bigfix Service Management provides predefined roles for common user personas, including:

- Consumers
- Fulfillers
- Administrators

Each role comes with a predefined set of permissions. Customers can leverage these roles to tailor access to features and data within their instance, ensuring users have access appropriate to their responsibilities.

4.6 API Security

Programmatic access to data is secured through authenticated APIs over encrypted channels. Authentication is handled using JWT-based mechanisms, leveraging Bearer and Refresh tokens. All API traffic is encrypted using TLS, ensuring confidentiality and integrity during transmission. API keys and tokens are securely managed, with periodic rotation to minimize the risk of compromise. Access to APIs is governed by least-privilege principles, and rate-limiting is enforced to prevent abuse.

4.7 Data Encryption

HCL BigFix Service Management employs industry-standard encryption mechanisms to protect customer data both in transit and at rest, ensuring confidentiality, integrity, and security throughout the data lifecycle.

4.7.1 Encryption in Transit

All customer access to HCL BigFix Service Management instances is secured using Transport Layer Security (TLS) with AES 256-bit cipher suites. Key features include:

- Automatic redirection of all HTTP requests to HTTPS.
- Customer-managed TLS: Customers may configure their own DNS and TLS certificates for enhanced control.
- Inter-datacenter encryption: Data transmitted across cloud data centers is automatically encrypted at the physical layer before leaving secured facilities.

These measures ensure that data remains protected from interception or tampering during transmission

4.7.2 Encryption at Rest

Data stored within the HCL BigFix Service Management platform is encrypted using AES-256 encryption, including:

- Primary database storage
- Automated backups

- Archived data

Encryption keys used for securing data at rest are managed by AWS Key Management Service (KMS). These keys are:

- Securely stored and rotated at regular intervals
- Access-controlled to ensure only authorized services and personnel can use them
- Audited to maintain compliance with security and privacy standards

This ensures robust protection of stored data against unauthorized access or compromise.

4.7.3 Integration Encryption

To secure integrations with customer-owned systems, HCL BigFix Service Management recommends the use of encrypted communication channels. Key practices include:

- TLS 1.2 and above as a standard for all inbound REST-based integrations.
- For systems within the customer's private network, HCL BigFix Service Management provides a lightweight gateway component that can be deployed within the customer's perimeter. This gateway securely communicates with the HCL BigFix Service Management instance over an encrypted channel.
- Customers are encouraged to use end-to-end encryption for all integration points to maintain data confidentiality across systems.

4.8 Data Residency

HCL BigFix Service Management respects customer preferences and regulatory requirements regarding data residency. Customer data is stored in geographically appropriate data centers based on contractual agreements and compliance obligations. The cloud infrastructure used by HCL BigFix Service Management ensures:

- Regional isolation of customer data
- Compliance with local data protection laws
- Controlled data movement across regions, with customer consent where applicable

Customers may request specific data residency configurations during onboarding or contract negotiation. the customer's responsibility to ensure their Splunk instance is properly secured.

4.9 Information Disclosure & Third-Party Data Sharing

We use web analytics services to measure how customers engage with our products and identify improvement areas. We may combine the analytics with the information you provide us to update, expand or provide you with tailored information within our products. We do not sell, rent, or trade any customer information collected through the websites or platform with third-party or external vendors for promotional purposes.

4.10 Data Archival

HCL BigFix Service Management puts in place an archival process that shifts less frequently accessed data to an archive. Data archival is done for operational purposes and to ensure optimal instance performance through its lifecycle. Archived data resides in the same geographical location as the primary data and is made available to customers upon submitting a request through the HCLSoftware customer support portal. HCL BigFix Service Management takes care of the following considerations:

- Archival is done monthly, and it shifts closed transactions older than 12 months into an archive. ▪ Archived data is retained at no additional cost for up to 3 years. Customers can request an extended retention period for an additional fee.
- Transient data such as application logs, system logs, and system-generated notifications are overwritten fortnightly.

4.11 Data Backup

HCL BigFix Service Management employs a robust backup strategy to ensure data integrity, recoverability, and resilience against data loss or corruption.

Daily Snapshots

- Full snapshots of databases are taken daily.
- These snapshots are securely stored within the cloud service provider's network, leveraging encrypted storage mechanisms.
- Snapshots are retained for 7 days, ensuring a rolling window of recoverable data.

Security of Backup Data

- All backup snapshots are encrypted at rest using industry-standard encryption protocols.
- Access to backup data is strictly controlled and limited to authorized personnel only, following role-based access policies.
- Backup infrastructure is isolated from production systems to reduce the risk of unauthorized access or accidental modification.

4.12 Data Return and Destruction

Throughout the lifetime of the subscription, data can be exported using features available in the product or by setting up an integration with HCL BigFix Service Management. When the subscription ends, customers may place a request, within 30 days of contract expiry, to hand over the export of their data. Data is permanently deleted after 30 days of the expiry of the subscription.

5 Data Confidentiality

HCL BigFix Service Management is committed to ensuring the confidentiality of enterprise data, regardless of how customers classify or categorize their information. This commitment is upheld through a combination of robust processes, policies, and governance frameworks that guide the secure handling of customer data throughout its lifecycle.

5.1 Governance and Policy Framework

HCL BigFix Service Management operates under the HCL Global Privacy Policy, which is informed by internationally recognized privacy and data protection standards. These frameworks help ensure that customer data is handled in a lawful, fair, and transparent manner. Key influences include:

- European Data Protection Directive
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Asian Pacific Economic Cooperation (APEC) Privacy Framework
- Organization for Economic Cooperation and Development (OECD) Privacy Guidelines
- Generally Accepted Privacy Principles (GAPP)

These frameworks collectively guide HCL BigFix Service Management in implementing controls around data access, storage, transmission, and disposal, ensuring that confidentiality is preserved across all operational layers.

5.2 Data Handling Practices

- **Data Minimization:** Only the minimum necessary data is collected and retained to fulfill service obligations.
- **Access Controls:** Role-based access ensures that only authorized personnel can view or process sensitive data.
- **Encryption:** Data is encrypted both in transit and at rest using industry-standard protocols.
- **Audit Trails:** All access to sensitive data is logged and monitored to detect and respond to unauthorized activity.

5.3 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.

5.4 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: Business Email
- Personal Identification: First Name, Last Name, Full Name
- User Account Information: Login ID
- Browsing Information – Session Time and IP Address
- Business Unit name/Company/Customer Name
- Conversation chat data

5.5 PII Data

As a product we do not control the data stored in the application. However, for providing support, support organizations may collect and store 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 customer.

- **First Name/Last Name/Full Name** – Information of 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.
- **Business Email Address/Login ID** – Information of the end user from the customer for Business Email Address and Login ID for general maintenance, support, and to improve the Support Services for the customer.
- **Browsing Information** – **Session Time and IP Address** – 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 BigFix Service Management). 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.
- **Conversation chat data** – The chat data from the user comprises 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 in our AI application.

5.6 PII Minimization and Consent Controls

The product allows customers to configure a customizable disclaimer, which will be displayed as a notification within the Web interface to guide users on appropriate data usage. To prevent the ingestion of unnecessary PII data for conversation or Gen-AI use cases, this disclaimer explicitly can be used to instruct users not to enter personal or sensitive information unless required for the intended functionality.

For added protection, the product supports redaction of stored conversation data. Regular-expression-based redaction is available as a configurable feature to automatically detect and replace PII data elements with generic placeholders. Client-side input redaction can also be performed on the web interface before data is stored.

5.7 Chat Data

Chat data constitutes the majority of data that is being processed or stored for every conversation happening between the bot and the user. Each query or question asked by the user contributes to data that contains multiple variables and text that corresponds to a chat.

A collection of chats altogether will form a conversation. A conversation can include both user queries and the response from the platform.

- **User**: The chat data from the user comprises mostly the user query in the form of plain text. The user can type their query as part of the Chatbot interface, and the text will be captured and sent to platform core. Even though the platform supports voice in Chrome, the data that will be processed or stored will be text, as the voice will be converted into text by using text-to-speech.
- **User queries** generally should not have any sensitive or critical data as part of it. The platform, while being designed for the use cases, will not collect any sensitive information, but users may type anything as a query that might include sensitive information. This information is not extracted, processed, or stored but is kept for historical logs and training purposes only.
- **Chat Bot**: Chatbot data comprises responses to the user for every query or response provided by the user. The user query is mostly text, but chatbot response can be of multiple formats but limited to the format(s) enabled/supported for application instances (e.g.: document, spreadsheet, images, pdf etc). The response from the chatbot can be a direct solution to the query posted by the user or a question to collect further information. The response can also be data from integrations with multiple applications to gather related data.

6 Multi-Tenancy and Data Segregation

HCL BigFix Service Management is designed to support multi-tenancy, enabling multiple customers to be hosted on a shared instance while maintaining strict logical data separation. This architecture is ideal for Managed Service Providers (MSPs) and Shared Service Organizations seeking to serve multiple clients from a single deployment.

6.1 Tenant Representation

In HCL BigFix Service Management, each customer is represented by a Company record, which serves as the logical boundary for data segregation. Companies are categorized into two types:

- Consumer Company: Represents the end customer consuming services.
- Provider Company: Represents the entity delivering services to one or more Consumer Companies.

A Consumer Company may use its own support groups or leverage those of its associated Provider Company, depending on the service contract.

6.2 Data Segregation Features

The following features ensure robust data isolation in multi-tenant environments:

- **Company-Based Segregation:**
  Each customer has a unique Company record, which can be designated as a Provider, Consumer, or hybrid.
  - A Consumer Company can be linked to one or more Provider Companies.
  - A Provider Company can serve multiple Consumer Companies.
- **Scoped Data Ownership:**
  Data such as organizational structures, service catalogs, configuration items (CIs), and service level agreements (SLAs) are scoped to the Consumer Company and stored under its record.
- **Controlled Data Sharing:**
  When a Consumer Company is associated with a Provider Company, selected data becomes visible to the Provider based on the service contract. This ensures transparency while maintaining control over sensitive information.
- **Transaction Isolation:**
  Transactions (e.g., incidents, requests) created under one Consumer Company are not visible to other Consumer Companies.
  - Only associated Provider Companies can view and manage these transactions, as permitted by the contract.

7 Availability Management

The production instance (SaaS) of HCL BigFix Service Management is deployed across two Availability Zones, interconnected via a low-latency network. Each zone is designed to operate independently, ensuring isolation from failures in the other zone. This architecture helps maintain service continuity even in the event of localized infrastructure issues. The Availability is calculated for each contracted month. Customers can refer to their specific contracts for the commitments.

7.1 Disaster Recovery

For customers who opt for Disaster Recovery, HCL BigFix Service Management (SaaS) offers the following objectives:

- Recovery Point Objective (RPO): 1 hour
- Recovery Time Objective (RTO): 4 hours

HCL BigFix Service Management makes commercially reasonable efforts to meet these DR objectives, ensuring minimal data loss and timely recovery in the event of a major incident.

7.2 Monitoring and Incident Response

HCL BigFix Service Management employs state-of-the-art monitoring systems to track instance health 24x7x365. Alerts are actively monitored by support teams, who follow established Standard Operating Procedures (SOPs) to mitigate any risks to availability.

8 Compliance and Certifications

The HCL BigFix Service Management platform has the following compliance certification/attestation available:

- ISO 27001
- SOC 2 Type II
- CERT – IN

9 Governance Risk and Compliance

HCLSoftware's commitment to security is operationalized through a comprehensive Governance, Risk, and Compliance (GRC) program. This program ensures that HCL BigFix Service Management is developed, maintained, and operated in accordance with rigorous internal standards and is validated against globally recognized external benchmarks.

Security is not a separate phase but is deeply integrated into every stage of the development lifecycle. This Secure SDLC is aligned with industry best practices and standards. Key security activities and gates are embedded throughout the process:

- **Requirements & Planning**: A Data Privacy Assessment is conducted for all new features to ensure privacy-by-design principles are met.
- **Design**: Formal threat modelling exercises are conducted to identify and prioritize potential threats to the system's architecture. A secure design review is performed by the HCLSoftware Security team to assess the proposed architecture and controls against industry standards.
- **Development**: Developers utilize secure OWASP coding practices, supported by regular training. Code is subjected to multiple layers of automated analysis, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) to detect vulnerabilities in custom code and open-source dependencies.
- **Testing & Validation:** In addition to quality assurance testing, every major release of HCL BigFix Service Management undergoes internal penetration testing. Annually, the platform is subjected to a comprehensive penetration test conducted by an independent, third-party security firm to provide an unbiased assessment of its security posture.
- **Maintenance:** 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 BigFix AEX can be found on the official HCL Software support and community forums.
- **Periodic Review of Cloud Infrastructure**: Regular evaluations of the underlying cloud infrastructure help identify configuration drift, performance bottlenecks, and emerging threats.
- **Internal Security Compliance Audits**: Scheduled internal audits ensure adherence to security policies, operational procedures, and regulatory requirements.
- **Automated and Manual Code Reviews**: Code is reviewed both automatically (via static analysis tools) and manually to detect vulnerabilities, enforce coding standards, and ensure secure development practices.
- **Automated and Manual Functional Testing**: Functional tests validate that features behave as expected and do not introduce security or stability risks.

- **Periodic Vulnerability Scans**: Regular scanning of the application and infrastructure helps identify known vulnerabilities and misconfigurations.
- **Annual Penetration Testing by Independent Firm**: External security experts conduct penetration tests to simulate real-world attack scenarios and uncover potential weaknesses.

10 Responsible AI Usage

Artificial Intelligence (AI) plays a transformative role in enhancing the capabilities of HCL BigFix Service Management, enabling smarter decision-making, automation, and improved user experiences. As AI technologies continue to evolve, we remain committed to ensuring that their integration into our platform is guided by ethical, transparent, and responsible practices. This document outlines our approach to responsible AI usage and provides guidance for users and stakeholders interacting with AI-powered features.

10.1 Ethical Foundations

At the heart of our AI strategy is a commitment to fairness, transparency, accountability, privacy, and safety. We believe that AI should serve all users equitably, without reinforcing bias or discrimination. To support this, our models are trained on identified datasets and are regularly evaluated to detect and mitigate any unintended bias and drift. We strive to ensure that AI-generated outputs are consistent, reliable, and respectful of the diverse contexts in which they are used.

Transparency is another cornerstone of our responsible AI framework. Our goal is to ensure that users have a clear understanding of how AI features function within the platform. AI-generated outputs are explicitly labelled, and we strive to provide documentation and contextual guidance to help users interpret and use these outputs effectively. We are committed to improving clarity over time by enhancing user education, offering accessible explanations where feasible, and maintaining openness about the capabilities and limitations of AI features. Transparency also means being honest about what AI can and cannot do and ensuring that users are empowered to make informed decisions when interacting with AI-driven functionalities.

Accountability is embedded in our development and operational processes. We maintain logs for AI-driven actions, enabling review. Users are encouraged to report any anomalies, inaccuracies, or concerns through our feedback channels, and we take these reports seriously as part of our continuous improvement efforts.

Privacy and data protection are integral to our responsible AI practices. Our systems are built to respect the boundaries of client data ownership and confidentiality. We ensure that data provided by one client is not used to train or improve models for general use, nor is it shared or leveraged to generate predictions for other clients. Each client's data remains isolated and is used strictly within the context of their own environment. This approach helps maintain trust, ensures data integrity, and supports compliance with contractual and regulatory obligations. Our AI features are designed to minimize data exposure, and users retain control over their data, including the ability to opt out of certain AI functionalities when appropriate.

Reliability and safety are essential to building trust in AI systems. Before deployment, our models undergo rigorous testing to validate their performance under various conditions. We implement safeguards to handle

unexpected behaviour and ensure that fallback mechanisms are in place to maintain system stability. Continuous monitoring helps us maintain high standards of accuracy and responsiveness.

10.2 User Responsibilities

While we take extensive measures to ensure responsible AI usage, users also play a vital role. We encourage users to critically evaluate AI-generated outputs, especially in scenarios where decisions may have significant consequences. It is important to use the provided feedback tools to report any issues or inconsistencies, as this helps us refine and improve our models. Users should also avoid submitting sensitive or confidential data unless explicitly supported and protected by the platform's security features. Staying informed about how AI features work and evolve is key to using them effectively and responsibly.

10.3 AI Usage Categories in HCL BigFix Service Management

In HCL BigFix Service Management, Artificial Intelligence capabilities are broadly classified into two categories based on their functional purpose:

10.3.1 Predictive AI

This category encompasses AI models designed to analyse historical and real-time data to identify patterns, forecast outcomes, and support proactive decision-making. These models typically operate on structured data and are integrated into the lifecycle of requests to enhance operational efficiency and responsiveness.

10.3.2 Generative AI

Generative AI refers to models that produce new content or responses based on input data, often in natural language or other unstructured formats. These capabilities are used to augment user interactions, automate content creation, and improve accessibility and engagement across the platform.

As our platform evolves, new AI-powered features may be introduced under either category. This classification helps maintain clarity around the nature of AI functionalities and supports consistent governance and responsible usage practices.

10.4 AI/ML Security Controls

10.4.1 AI Governance & Risk

- **AIMS scope and policy** – Follows HCLSW AI policy and scope for the AI Management System (AIMS) with defined accountable roles and human oversight for safety-critical use cases.
- **AI risk register** – Risk register covering data poisoning, model theft, inference leakage, and over-reliance risks.

10.4.2 Data & Training

- **Provenance and licensing** – Enforced dataset lineage and consent checks, attesting training sets before use.

- **Poisoning defences** - Schema/semantic validation, canary datasets, outlier and label-flip detectors, treating as a pre-train gate.

10.4.3 Model Integrity & Robustness

- **Model registry security**: Stores models in an access-controlled registry, signed model artifacts and serving images.
- **Adversarial testing**: Testing against evasion, extraction, inversion, and backdoors.

10.4.4 Operations & Runtime

- **Service-to-service trust** Mutual TLS and fine-grained authorization between data pipelines and model serving.
- **Security telemetry for AI** Correlating drift with security anomalies (e.g., atypical input distribution).

10.4.5 Credential and Secret Security

- Service credentials stored using hashing with unique salts.
- The use of a unique salt for each secret is critical. It ensures that even if two services had the same password, their stored hashes would be completely different, preventing attackers from identifying duplicate passwords.

10.4.6 ML Model Protection

- Encryption of all trained model files
- **Model Obfuscation**: Complexity added to make reverse-engineering difficult
- **Digital Watermarking**: Embedded identifiers for intellectual property protection

10.4.7 API & Model Access Security

- **API Key Management**: API keys are securely generated and rotated.
- **Scoped Access**: APIs are protected with least-privilege permissions and rate-limiting to avoid abuse or overuse

10.4.8 Responsible AI and Ethical Safeguards

- **Explainability**: All outputs are traceable with logs and model outputs are explained to the users.
- **Bias Detection**: Models provide statistics for fairness and bias regularly

10.5 Secure MLOPs Lifecycle Management

10.5.1 Data Sourcing & Preparation

- Access control to data sources via RBAC
- Automated data provenance and lineage tracking
- Data poisoning prevention through schema validation and anomaly detection

10.5.2 Model Training

- Encrypted communication for distributed training nodes
- Adversarial robustness testing to pre-empt evasion attacks

10.5.3 Model Deployment

- All deployments containerized with minimal base images
- Deployment policies enforce runtime security constraints

10.6 Model Governance

10.6.1 Model Lifecyle Management

- **Version control**: Tracking different versions of models, datasets, and features.
- **Lineage tracking**: Recording data sources, transformations, training parameters.

10.6.2 Data Governance

- **Data quality monitoring**: Checking for missing, corrupt, or skewed data.
- **Data lineage**: Traceability from raw sources to model inputs.
- **Privacy compliance**: Ensuring privacy is respected (e.g., through anonymization, consent logging).

10.6.3 Model Explainability & Interpretability

- Use of integrated model-specific explainers.
- Model Cards

10.6.4 Fairness & Bias Monitoring

- Pre- and post-deployment bias checks across attributes (gender, race, etc.).
- Fairness metrics: e.g., equal opportunity difference, demographic parity.

10.6.5 Model Performance Monitoring

- Drift detection: Concept and data drift.
- Performance degradation tracking: E.g., AUC, F1-score over time.

10.6.6 Auditability & Traceability

- Comprehensive logging: Who trained what, when, using which data and parameters.
- Audit trails: For external compliance and internal accountability.

10.6.7 Access Control & Security

- RBAC: Role-based access control on models and datasets.
- Model encryption and secure deployment.
- Secure APIs and access tokens for inference.

10.6.8 Retraining & Lifecycle Refresh

- Triggered by performance decay or data drift.
- Appropriate role needed for retraining.
- Tracking retraining logic, triggers, and audit logs.

.

11 Conclusion

HCL BigFix Service Management is built with security, privacy, and trust at its core. Through rigorous controls, continuous monitoring, and adherence to global standards, we ensure that customer data is protected throughout its lifecycle—from ingestion and processing to archival and deletion.

Our commitment to responsible AI usage, secure multi-tenancy, and transparent data governance reflects our dedication to building a platform that not only meets technical and regulatory requirements but also earns the confidence of our users. As threats evolve and technologies advance, HCL BigFix Service Management remains focused on delivering secure, resilient, and ethically governed services that empower organizations to operate with assurance.

For further details or specific inquiries, customers are encouraged to reach out through the HCL Product Support portal or consult their contractual documentation.

12 Support

For more information and related queries drop an email to hclbigfixsm-pmg@hcl-software.com

HCLSoftware

hcltechsw.com