BOUSTEAD
Geospatial Technologies

Trust and Security

GEOVONIC$^{\text{TM}}$ CONNECT FOR ArcGIS®

Author: Gary Johnson

Report Date: 11 September 2025

DOCUMENT INFORMATION

Document Status

Release Status	Final
Approval Date	11 September 2025

Document Change Control

Version	Release Date	Authors	Change Summary
1.0	11 Sep 2025	Gary Johnson	Initial Version

TABLE OF CONTENTS

1 SUMMARY

Geovonic™ Connect for ArcGIS® is an easy-to-use extension for users of ArcGIS web mapping applications, allowing your users to surface information and interact with your business systems via a map-driven interface, with no custom coding required.

Using the Geovonic Connect for ArcGIS widget, Experience Builder application authors can provide capabilities for users to view data that is retrieved in real-time from third-party applications and databases based on feature selections on a web map, launch business systems directly from a map feature, and generate reports combining information from both the map and your applications.

1.1 Purpose of this Guide

The Trust and Security Guide outlines how Boustead Geospatial Technologies (BGT) and Geovonic Connect for ArcGIS ensure the confidentiality, integrity, and availability of customer data. It is designed to give customers, partners, and auditors a clear understanding of the security practices, compliance certifications, and architectural decisions that underpin the platform.

1.2 Commitment to Trust and Security

At BGT, trust is foundational. We recognise that our customers rely on Geovonic Connect to securely integrate geospatial systems with enterprise platforms. Security is not an afterthought, but a core principle embedded into our product design, development lifecycle, and daily operations. This commitment extends to:

- Maintaining compliance with recognised international security standards.
- Applying best practices in cloud architecture and service design.
- Continually monitoring, assessing, and improving our security posture.
- Providing transparency into how data is managed and protected.

1.3 Scope

This document covers the key aspects of trust and security in Geovonic Connect, including:

- **Information Security Management:** Our alignment with ISO/IEC 27001 and risk management framework.
- **System Architecture:** How the platform is designed for resilience, security, and scalability.
- **Geovonic Relay Service:** The secure middleware layer that connects ArcGIS with third-party systems.

- **Data Security and Privacy:** Policies for encryption, retention, and compliance.
- **Identity and Access Management:** Mechanisms for secure authentication and access control.
- **Operational Security:** Our approach to vulnerability management, incident response, and ongoing assurance.

This guide is not intended to provide detailed technical specifications or configuration manuals. Instead, it offers a high-level overview of the measures and frameworks we use to protect customer data and maintain trust.

2 INFORMATION SECURITY MANAGEMENT

2.1 ISO/IEC 27001:2022 Accreditation

BGT operates under an **ISO/IEC 27001:2022-certified Information Security Management System (ISMS)**. This internationally recognised standard provides a structured framework for managing information security risks and implementing controls to protect customer data.

- **Certification Overview**

Our ISO/IEC 27001:2022 accreditation demonstrates that we follow a systematic approach to managing sensitive information, applying the principles of confidentiality, integrity, and availability (CIA). Certification is maintained through regular independent audits.

- **Controls Framework**

The ISMS is aligned with ISO/IEC 27001:2022 Annex A controls, which cover areas such as:

- Access control and authentication
- Cryptography and encryption practices
- Physical and environmental security
- Secure development and change management
- Supplier and third-party risk management
- Incident management and response procedures

- **Continuous Improvement and Audits**

Compliance is not a one-off activity. Our ISMS is regularly reviewed, audited, and updated to adapt to emerging threats, evolving regulations, and feedback from internal and external assessments.

2.2 Risk Management Approach

Risk management is at the core of our security strategy. BGT applies a risk-based approach to identify, assess, and mitigate threats to data and services.

- Threat modelling is conducted during system design.
- Risks are classified by likelihood and impact, and mitigation measures are applied proportionally.
- Residual risks are reviewed by senior management as part of the ISMS governance process.

This ensures that security investments are aligned with the most critical risks to customer data and service continuity.

2.3 Data Protection and Privacy Commitments

Geovonic Connect is built to support compliance with global data protection and privacy regulations, including GDPR and regional data residency requirements.

Key commitments include:

- Data minimisation: Only necessary data is collected, processed, and retained.
- Encryption: All customer data is encrypted both in transit and at rest using industry-standard protocols.
- Privacy by design: Security and privacy controls are embedded into product development and architecture decisions.
- Customer transparency: Customers can request details on how their data is processed, where it is stored, and how long it is retained.

2.4 Governance and Accountability

The ISMS is overseen by a designated Information Security Officer (ISO) and supported by a cross-functional security governance team. Roles and responsibilities are clearly defined to ensure accountability for maintaining the highest security standards.

- Security policies are reviewed annually.
- Employees undergo mandatory security awareness training.
- All staff and contractors are bound by confidentiality agreements.

3 SYSTEM ARCHITECTURE

3.1 High-Level Overview

Geovonic Connect for ArcGIS is delivered as a **cloud-native integration platform**, designed for scalability, resilience, and security.

- Hosted on **Amazon Web Services (AWS)**, leveraging its global infrastructure.
- Integrates securely with **ArcGIS Online/Enterprise** and third-party business applications (e.g., ServiceNow, Salesforce).
- Employs a **multi-tier architecture** separating presentation, application logic, and data layers to reduce risk and improve performance.

3.2 Core Components

- **Geovonic Connect Widget:** Provides end-user facing functionality for the ArcGIS user to fetch data, trigger workflows, and generate reports. Authentication uses the user’s ArcGIS credentials.
- **Geovonic Connect Application Layer:** Manages integration logic, workflows, and connectors.
- **Data Services Layer:** Manages temporary caching, logs, and metadata in line with retention and encryption policies.
- **Geovonic Relay Service:** (Optional) Acts as a secure middleware layer for API requests between ArcGIS and external systems (covered in detail in Section 4).
- **Hosted Experience Builder:** (Optional)
- **Monitoring and Logging:** Cloud-native tools (e.g. AWS CloudWatch, Pingdom) provide continuous observability, with integration to Jira Service Management.

3.3 Context Diagram

The following diagram shows the core components of the Geovonic Connect solution and the connections to integrated systems. The notes below refer to the numbered items on the diagram.

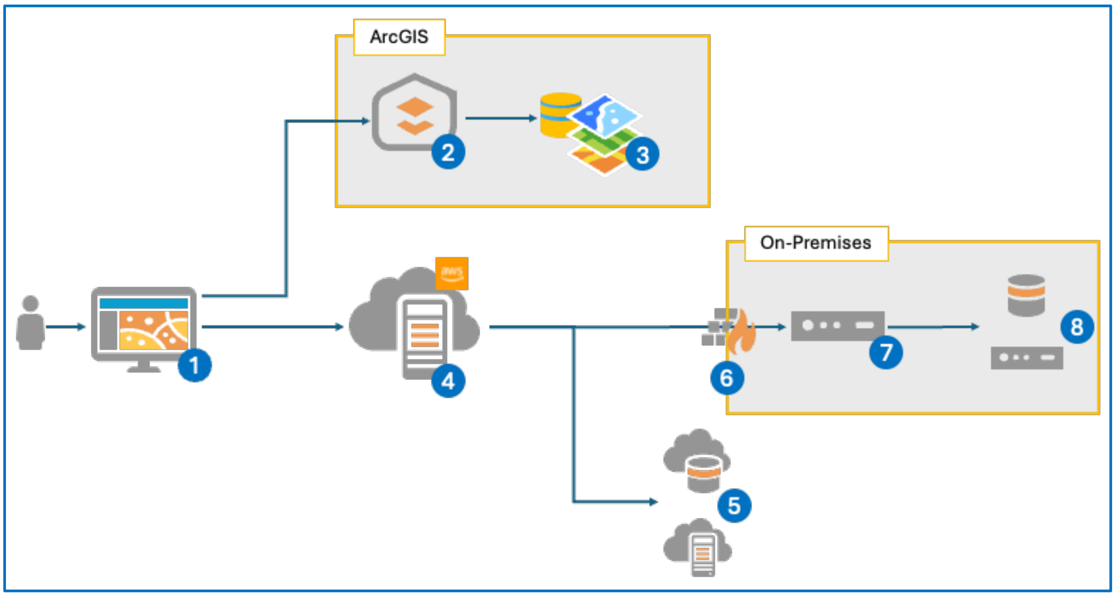

Figure 1 - Solution Architecture Diagram

1. The user authenticates to your ArcGIS environment (2) and launches an Experience Builder app. The app includes the Geovonic Connect widget. The widget makes requests to the Geovonic Connect cloud environment (4) to fetch data or trigger workflows.
2. The ArcGIS Portal (ArcGIS Online or ArcGIS Enterprise) is responsible for authenticating users. Group memberships are used to authorise access to integrations configured in Geovonic Connect.
3. All mapping data and services resides in the ArcGIS data store. Requests for mapping data and services are direct from Experience Builder to ArcGIS – standard data requests do not flow through Geovonic Connect (4). (Note: if using the Feature Layer Enrichment feature, mapping data is proxied via the Geovonic Connect cloud).
4. The core Geovonic Connect components run in the Amazon Web Services cloud. Processing uses a combination of Lambda serverless functions and Elastic Container Service auto-scaling tasks. Storage uses RDS for persistent data, S3 for report templates, and DynamoDB for ephemeral data. If using the hosted Experience Builder, the app configuration files are stored in Elastic File Storage.
5. Third-party systems and databases available from the public internet (or via IP whitelisting) are called from Geovonic Connect (4) using the protocol of the target system.
6. When connecting to systems and databases that are running on-premises, Geovonic Connect (4) will need to navigate the firewall using the Geovonic Relay Service (7).
7. The Geovonic Relay Service acts as a data gateway agent running within the secure zone. The relay service opens up a secure bi-directional web socket to Geovonic Connect (4).
8. Requests to on-premises systems and databases (8) are forwarded by the relay service. The on-premises systems and databases respond to the requests and the response records are returned via the Relay Service.

3.4 Data Flow and Security Boundaries

- **Inbound Connections:** All customer access is authenticated via ArcGIS (see Section 6).
- **Data Transit:** Encrypted using TLS 1.2+ with strict cipher policies.
- **Data Processing:** Integration logic runs in isolated execution environments, ensuring tenant separation.
- **Outbound Connections:** Requests to third-party systems follow the security mechanisms available in the destination applications and database.

3.5 Segregation of Environments

- **Development, QA, Production:** Strictly segregated to prevent cross-environment data leakage.
- **Access Control:** Only authorised personnel can access production, with activity logged and reviewed.
- **Change Management:** Infrastructure-as-Code (IaC) ensures consistency across environments.

3.6 Availability, Reliability and Resilience Design

- **High Availability:** Services are deployed across multiple AWS availability zones to protect against localised failures.
- **Auto-Scaling:** Application layer scales horizontally to handle demand surges.
- **Disaster Recovery:** Combined with RDS point-in-time recovery (see Section 5), ensuring resilience against failures.
- **Service Isolation:** Relay services and connectors are isolated to prevent cascading failures.

3.7 Monitoring and Logging Practices

- **Real-Time Monitoring:** Cloud-native monitoring tracks performance, availability, and security events.
- **Alerts:** Automated alerts trigger escalation to the operations team in the event of anomalies.
- **Audit Logging:** All critical system events are logged and retained per compliance standards.

4 GEOVONIC RELAY SERVICE

4.1 Purpose and Function

The **Geovonic Relay Service** is a lightweight **gateway agent** deployed within the customer's network (behind the firewall). It establishes a **single outbound, TLS-protected WebSocket (wss)** to the Geovonic Connect cloud, enabling **secure, two-way communication** without opening inbound firewall ports or exposing internal services publicly.

Key properties:

- **Outbound-only connectivity:** No inbound exposure; compatible with corporate proxies.
- **Two-way messaging:** Cloud-initiated requests (e.g., callbacks, data pulls) are multiplexed over the secure WebSocket to on-prem systems through the agent.
- **Deterministic egress:** Traffic egresses only to documented Geovonic endpoints over port 443.

4.2 Context Diagram

The following diagram describes the implementation of the Geovonic Relay Service and how it creates a secure connection from on-premises systems to the Geovonic Connect cloud. The notes below refer to the numbered items on the diagram.

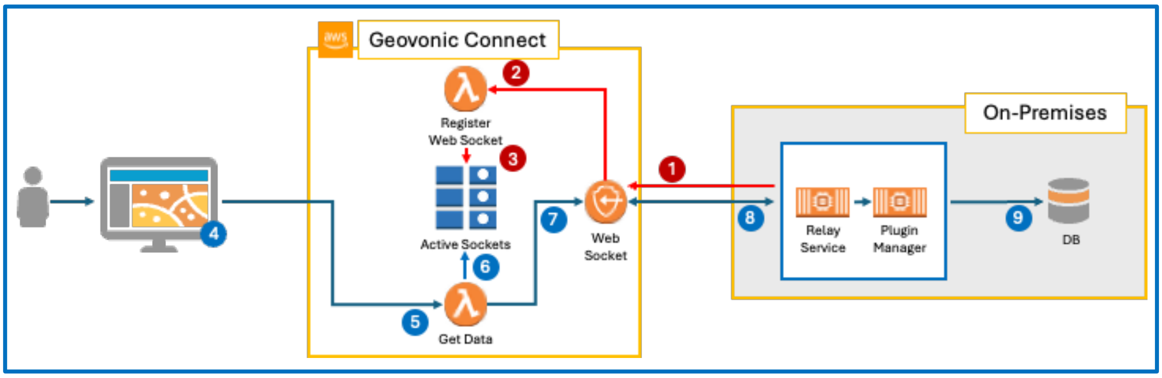

Figure 2 - Relay Service Context Diagram

1. The Relay Service runs as a Windows service within the on-premises secure environment. On start-up, the Relay Service attempts to open a secure web socket connection to the Geovonic Connect cloud. The web socket connection request includes an authorisation header and tenant identifier. The authorisation header contains the current server time encrypted using the client's public key.
2. A Lambda function in the Geovonic Connect cloud authenticates the web socket request. The web socket connection will only be accepted if the authorisation header can be decrypted using

the subscriber’s private key held by the Relay Service server. If the connection fails authentication, the web socket is immediately dropped.

3. After successful authentication, the web socket reference information is stored in a DynamoDB table linked to the tenant organisation. This table is used to identify the web socket connection for future data requests.
4. When a user makes a data request or triggers a workflow from the Geovonic Connect widget, an API call is sent to the Geovonic Connect API gateway. All requests include the user’s JWT token for authentication.
5. On receipt of the API call, a Lambda function checks the data source configuration to determine if the request should be sent via the Relay Service.
6. A DynamoDB query finds the web socket reference information for the user’s tenant organisation.
7. The request details are sent via the web socket to the Relay Service. Every message sent from the Relay Service server via the web socket to the client is signed using the private key.
8. The Relay Service client verifies the signature using its public key before accepting the message. Any message received through the web socket that does not carry a verified signature is rejected. The signature is created using SHA256 RSA asymmetric encryption method.
9. A request is made to the target system or database using the target’s protocol. The response data is returned via the web socket and packaged into a response to return to the user (4).

4.3 Identity, Authentication, and Signing

- **Asymmetric key identity:** Each agent is provisioned with a 2048-bit RSA **public/private key pair**; the **private key** is registered with Geovonic Connect to establish agent identity and the **public key** is installed with the relay service.
- **Mutual verification:** On connection, the agent proves possession of the private key; the platform validates the corresponding public key.
- **Request signing:** All agent-originated requests and sensitive message envelopes are **digitally signed** to ensure **integrity and non-repudiation**. Signatures are verified in the cloud and by the on-prem agent.
- **Key lifecycle:** Procedures exist for **rotation, revocation, and re-enrolment** of agent keys.

4.4 Encryption

- **Transport:** All traffic uses **TLS 1.2+** over **wss** with modern cipher suites.
- **Message integrity: Digital signatures** protect messages against tampering on the wire and at rest within transient queues.

- **Secrets handling:** The agent avoids storing long-lived credentials where possible (dependent on the capabilities of the target business systems).

4.5 Isolation and Resilience

- **Tenant isolation:** Logical isolation per customer and per connector; no cross-tenant data paths.
- **Service isolation:** Connectors execute in segregated contexts to limit blast radius.
- **Resilience:** Automatic **reconnect**, **backoff**, and **resume** to handle transient outages.
- **Remote patching:** Patches to business system connectors are automatically deployed to the customer environment, ensuring customers do not need to manually patch the integration connectors.

4.6 Deployment Considerations

- **Network:** Outbound HTTPS (443) to Geovonic Connect.
- **Host:** Runs as a service or container on Windows with minimal footprint.
- **Registration:** Agent configuration is downloaded from the Geovonic Connect administration console including secure keys unique to the customer environment.
- **Change control:** Patches are pulled from the cloud over the secure channel and applied automatically.

4.7 Customer Benefits

- **No inbound firewall changes** and no public exposure of internal systems.
- **Cryptographic identity and signed requests** for strong trust guarantees.
- **Resilient, low-latency** path for bi-directional workflows between Geovonic cloud and on-premises systems.

4.8 Installation

The Geovonic Relay Service is downloaded as a ZIP file from the Geovonic Connect admin console. The ZIP file contains the executable code as well as a tailored configuration file for the tenant organisation.

The Relay Service should be installed on a server within the secure environment and must have access to the ports required to reach the target systems and databases.

Installing the Relay Service requires administrator access to install and run the two Windows services.

1. Unzip the **GeovonicRelayService.zip** file to your target folder.
2. Open a command prompt as an administrator and navigate to the target folder.
3. Run the following commands: -

   ```
   PluginService.exe install

   PluginService.exe start

   RelayService.exe install

   RelayService.exe start
   ```

4. The dashboard in the Geovonic Connect admin console will show a Connected status for the Relay Service once a secure connection has been created.

Once installed, you can check the status and start/stop/restart the Relay Service via the Services management console.

The Relay Service can be uninstalled by entering the following commands: -

```
RelayService.exe stop

RelayService.exe uninstall

PluginService.exe stop

PluginService.exe uninstall
```

5 DATA SECURITY

5.1 Data Classification and Handling

Geovonic Connect applies a **data classification framework** to ensure that information is handled appropriately based on its sensitivity.

- **Customer Data:** Business and geospatial information exchanged via integrations.
- **System Data:** Logs, configuration details, and telemetry required for service operation.
- **Confidential Data:** Credentials, API keys, and identity-related tokens.

Each category is subject to tailored controls around storage, access, and retention.

5.2 Encryption Standards

All data is encrypted both **in transit** and **at rest** to ensure confidentiality and integrity.

- **In Transit:** Encrypted with TLS 1.2+ using strong cipher suites.
- **At Rest:** Encrypted using AES-256 or equivalent standards, applied to databases, backups, and object storage.
- **Key Management:** Managed through the AWS Key Management Service (KMS) with strict access controls and rotation policies.

5.3 Storage and Retention Policies

- **GIS Data:** Geovonic Connect does not store or copy any GIS data. Experience Builder applications directly consume services coming from your ArcGIS environment. Some system plugins may perform queries against your GIS web services but no data is stored.
- **Third-Party System Data:** Geovonic Connect does not store or copy your third-party system data. The Geovonic Connect administrator may choose to enable caching in the layer link configuration. When enabled, query results will be cached within Geovonic Connect for the maximum time-to-live specified by the administrator. The cached results are automatically purged after the time-to-live expiry or on demand by administrator action.
- **Retention Periods:** Customer configuration data is retained only for as long as it is required to provide services or as contractually agreed.
- **Data Minimisation:** Temporary files, cached results, and logs containing sensitive data are automatically purged within defined timeframes.
- **Secure Disposal:** When data reaches end-of-life, it is securely deleted by Amazon Web Services following NIST 800-88 guidelines.

5.4 Backup and Disaster Recovery

Geovonic Connect maintains a robust backup and recovery strategy to protect against accidental loss, corruption, or disaster scenarios.

- **Continuous Backups:** AWS RDS provides point-in-time recovery, enabling restoration to five-minute intervals over the last 7 days.
- **Automated Snapshots:** Regular backups of critical databases and configurations: -
  - Weekly backups retained for 5 weeks.
  - Monthly backups retained for 13 months.
  - Yearly backups retained for 7 years.
- **Immutable Backups with AWS Backup Vaults:** Backup policies are enforced through AWS Backup Vaults, which support immutability and access controls to prevent tampering or deletion of backups. This ensures compliance with retention requirements and adds an extra layer of resilience against ransomware or insider threats.
- **Redundancy:** Data replicated across multiple availability zones. The RDS configuration uses real-time replication to a standby node in a separate data centre to handle automatic failover for component or site loss.
- **Disaster Recovery (DR):** Tested DR plans ensure recovery time objectives (RTO) and recovery point objectives (RPO) aligned with business continuity requirements.

5.5 Customer Data Ownership

Customers always retain **full ownership** of their data. Geovonic Connect acts as a **data processor**, ensuring that data is never shared, sold, or repurposed outside the agreed scope of service delivery.

6 IDENTITY AND ACCESS MANAGEMENT

6.1 Authentication

All logins to **Geovonic Connect** are handled through **ArcGIS authentication**. This ensures:

- Customers leverage their existing ArcGIS Online or ArcGIS Enterprise identity provider.
- No separate password database is maintained by Geovonic Connect, reducing risk and administrative burden.
- Security policies (e.g., password rotation, single sign-on) remain under the customer's control.

6.2 Multi-Factor Authentication Support

Because authentication is delegated to ArcGIS, customers can enforce MFA and other advanced identity protections directly within their ArcGIS environment. This provides flexibility to align with organisational policies without requiring Geovonic Connect to manage MFA configurations.

For more details, please refer to the ArcGIS Architecture Center documentation.

6.3 Role-Based Access Control

Within Geovonic Connect, access to functionality and configuration is governed by **role-based access controls (RBAC)**. These roles map to ArcGIS-authenticated user identities, ensuring that:

- Only authorised users can configure integrations or manage sensitive settings.
- Permissions can be aligned with organisational responsibilities (e.g., administrators vs. data consumers).
- Integrations can be configured to be available based on ArcGIS groups, allowing group-based authorisation through the customer's ArcGIS environment.

6.4 Least Privilege Principle

User access is restricted to the **minimum level of permissions** required to perform their role. Administrative actions are logged and monitored.

7 COMPLIANCE AND PRIVACY

7.1 Regulatory Alignment

Geovonic Connect is designed to support compliance with global and regional data protection regulations, including:

- **GDPR (General Data Protection Regulation)** for customers operating in the European Union.
- **CCPA (California Consumer Privacy Act)** for customers in California, USA.
- **Australian Privacy Principles (APPs)** for customers in Australia.
- Other region-specific frameworks as required by customer contracts.

The platform's security and privacy controls are regularly reviewed against these regulations to ensure ongoing alignment.

7.2 Data Residency Options

Customers may have specific requirements for where their data is stored and processed. Geovonic Connect supports **data residency options** through the use of AWS regional services.

- Data is stored in the AWS region selected by the customer when launching their subscription.
- Integration data and backups never leave the selected region unless explicitly requested by the customer.
- Logs and monitoring data are likewise retained in-region to maintain compliance.

7.2.1 Region Options

The customer may choose between the following regions: -

- **Australia**: All processing and data storage is within the AWS Sydney region (ap-southeast-2).
- **United States**: All processing and data storage is within the AWS Ohio region (us-east-2).
- **Europe**: All processing and data storage is within the AWS Frankfurt region (eu-central-1) region.

7.3 Privacy by Design

Privacy considerations are embedded in the product lifecycle. Key practices include:

- **Data Minimisation:** Only the minimum data required to provide functionality is collected and processed.

- **Pseudonymisation/Tokenisation:** Where applicable, sensitive identifiers are replaced with tokens to reduce risk.
- **Access Transparency:** Customers can request logs to show who accessed their data and when, through logging and audit trails.

7.4 Third-Party and Vendor Risk Management

Geovonic Connect relies on trusted third-party services (e.g., Amazon Web Services for hosting, ArcGIS for authentication). These providers are assessed and monitored to ensure their compliance with industry standards.

- AWS maintains compliance with ISO 27001, SOC 2, and other major certifications.
- Esri maintains certifications for ArcGIS Online and ArcGIS Enterprise environments.
- Vendor contracts include data protection and confidentiality provisions.

7.5 Customer Rights and Responsibilities

Geovonic Connect ensures customers can exercise their rights under applicable data protection laws, including:

- The right to access, correct, or delete personal data.
- The right to request information about where and how data is processed.
- The right to restrict or object to certain processing activities.

Customers are responsible for configuring their **ArcGIS identity provider** and **integration settings** in line with their own regulatory requirements.

8 OPERATIONAL SECURITY

8.1 Secure Software Development Lifecycle

Geovonic Connect is developed following a **secure-by-design philosophy**. Security is integrated at every stage of the development lifecycle:

- **Design:** Threat modelling and security requirements defined before coding begins.
- **Development:** Code quality tools, static application security testing (SAST), and peer reviews ensure vulnerabilities are identified early.
- **Testing:** Dynamic application security testing (DAST) and dependency scanning are performed on a quarterly basis.
- **Deployment:** Infrastructure as code (IaC) templates are security-hardened and reviewed before deployment.

8.2 Vulnerability Management and Penetration Testing

We follow a proactive approach to identifying and mitigating vulnerabilities:

- **Automated Scanning:** Regular scans of code, dependencies, and container images.
- **Patch Management:** Critical security patches applied within industry-recommended timelines.
- **Penetration Testing:** Independent third-party penetration tests are performed annually, with findings remediated promptly.

8.3 Incident Detection and Response

Geovonic Connect maintains an **incident response plan** aligned with ISO/IEC 27001:2022 and industry best practices.

- **24/7 Monitoring:** Cloud-native tools such as AWS CloudWatch and Pingdom provide continuous monitoring for anomalies and threats.
- **Response Procedures:** Documented runbooks guide detection, containment, eradication, and recovery actions.
- **Communication:** Customers are notified promptly of any confirmed incidents that affect their data, with regular updates provided until resolution.
- **Post-Incident Review:** Lessons learned are documented and integrated into process improvements.

8.4 Change and Configuration Management

- **Change Control:** All production changes are logged, peer-reviewed, and approved before implementation.
- **Configuration Management:** Infrastructure is managed as code, ensuring repeatability and minimising configuration drift.
- **Separation of Duties:** Development, testing, and production environments are strictly segregated.

8.5 Employee Training and Awareness

- **Mandatory Training:** All employees undergo regular security awareness training, with additional sessions for developers on secure coding practices.
- **Access Controls:** Staff access to production environments is limited to a small group of authorised engineers and logged at all times.
- **Background Checks:** Employees with access to sensitive systems undergo pre-employment screening.

9 CUSTOMER RESPONSIBILITIES

Security and compliance within BGT and Geovonic Connect follows a **shared responsibility model**. While BGT and Geovonic provides secure infrastructure, managed services, and operational controls, customers retain responsibility for configuring and using the platform in a secure and compliant manner.

9.1 Identity and Access Control

- Customers must configure **ArcGIS authentication** according to their organisational policies, including enabling **multi-factor authentication (MFA)** where required.
- Role-based access control (RBAC) within Geovonic Connect should be aligned with business roles to enforce the **principle of least privilege**.
- Customers are responsible for managing user lifecycle events (e.g., onboarding, offboarding, access reviews).

9.2 Data Governance

- Customers retain **full ownership** of their data. It is their responsibility to ensure that data uploaded, shared, or integrated via Geovonic Connect complies with applicable laws and organisational standards.
- Customers must classify and protect their data appropriately, especially when handling sensitive or regulated information.
- Data exported or integrated into third-party systems falls under the security and compliance scope of those systems.

9.3 Integration Security Considerations

- When connecting Geovonic Connect to external applications and databases, customers must ensure those endpoints are properly secured.
- Customers should configure API keys, tokens, and credentials with **least privilege** access and rotate them periodically.
- Third-party integrations must be vetted to confirm they meet the organisation’s security requirements.

9.4 Operational Practices

- Customers are responsible for maintaining compliance with their own regulatory obligations (e.g., GDPR, HIPAA, CCPA) when using Geovonic Connect.

- Customers should regularly review configurations in Geovonic Connect to maintain organisational security standards.
- Incident reporting: If a customer becomes aware of a potential security incident involving Geovonic Connect, they should notify our support team immediately for coordinated response.

  Support and Security Contact: support@geovonic.com

9.5 Shared Responsibility Summary

- **BGT is responsible for:** platform security, infrastructure, service availability, encryption, monitoring, and compliance certifications.
- **Customers are responsible for:** authentication configuration, data governance, integration security, and adherence to applicable legal/regulatory frameworks.