# Service Definition: Security Services

## 1. Overview – What the Service Is

Security Services provide comprehensive protection for cloud-based systems, applications, and data against security threats while maintaining confidentiality, integrity, and availability. The service is designed to help organisations establish, operate, and continuously improve their security posture across cloud environments, ensuring that security controls remain effective as systems evolve.

These services support organisations at all stages of cloud adoption, from initial design through to day-to-day operations. Security Services integrate technical controls, monitoring, governance, and operational processes to reduce risk, support compliance, and respond effectively to security incidents.

---

## 2. Scope of the Service

Security Services typically include:

- Cloud security architecture and design
- Identity and access management support
- Network security and segmentation
- Security monitoring and threat detection
- Vulnerability assessment and remediation support
- Security configuration and hardening
- Compliance and audit support
- Security incident response and investigation

The service can be delivered as a standalone security function or integrated with cloud support and migration services.

## 3. Data Backup, Restore, and Disaster Recovery

Security Services support the protection of backup and recovery systems to ensure that data remains secure and recoverable during incidents. This includes ensuring that backups are protected against unauthorised access, tampering, or ransomware, and that recovery processes are tested and secured.

Security controls are applied to backup storage, access policies, and recovery workflows. Where required, guidance is provided on immutable backups, separation of duties, and secure recovery environments to reduce the impact of security incidents.

---

## 4. Onboarding and Offboarding Support

### Onboarding

Onboarding begins with a security assessment to understand the existing environment, risks, and regulatory requirements. Security baselines are defined, and roles and responsibilities are agreed.

Access to systems is established using least-privilege principles, with strong authentication and logging enabled. Security tools and integrations are configured as part of onboarding where applicable.

### Offboarding

Offboarding includes secure revocation of access, transfer of security documentation, and handover of security configurations and reports. Any temporary access or tooling is removed, and retained security data is handled in line with agreed retention policies.

---

## 5. Service Constraints

Security Services must operate within the technical and regulatory constraints of the underlying cloud platforms. Some security controls may be limited by platform capabilities or legacy application design.

Changes to security configurations follow controlled change management processes to avoid service disruption. Emergency security actions may be taken to mitigate active threats.

The service is typically delivered remotely.

---

## 6. Service Levels and Incident Response

Service levels define how security events are handled, including:

- Monitoring coverage and alerting
- Incident response times based on severity
- Escalation and communication procedures

Security monitoring operates continuously, and incidents are managed through defined response processes. Post-incident reviews are conducted to identify root causes and improvement actions.

---

## 7. After-Sales and Ongoing Security Support

Ongoing security support includes continuous monitoring, regular reviews of security posture, and proactive recommendations for improvement. This may include policy updates, control tuning, and support for new services or changes in the environment.

The service also supports audits, regulatory assessments, and compliance reporting as required.

---

## 8. Technical Requirements

To deliver Security Services effectively, the following are typically required:

- Integration with identity systems
- Access to logs and monitoring data
- Visibility into network and application configurations
- Collaboration with operational and development teams

All access is controlled, monitored, and reviewed.

---

## 9. Outage and Maintenance Management

Security changes are planned and tested to minimise operational impact. Where security actions may affect availability, stakeholders are informed in advance.

In the event of a security-related outage, response actions prioritise containment, recovery, and restoration of services, followed by investigation and reporting.

---

## 10. Hosting Options and Locations

Security Services support cloud environments hosted across public, private, and hybrid infrastructures. Security controls are designed to align with data residency and regulatory requirements in different regions.

---

## 11. Access to Data Upon Exit

Security logs, reports, and configurations are provided to the customer upon exit. Access credentials are revoked, and retained security data is returned or securely deleted in line with contractual and regulatory requirements.

---

BAYWATER CONSULTING
IMPROVEMENT SPECIALISTS

# 12. Security and Data Protection

The delivery of Security Services follows strict security and data protection practices. This includes:

- Strong identity and access controls
- Encryption of sensitive data
- Secure handling of logs and reports
- Regular auditing and review of access

The service itself is designed to uphold high standards of confidentiality, integrity, and availability, ensuring trust and transparency throughout engagement.