



GENERAL GUIDANCE ON G-CLOUD SERVICE DEFINITIONS

1 Preamble

This Document provides an overview service definition for Panlogic's best practice cloud security services included within G-Cloud. This document should be read in conjunction with the pricing, and/or terms and conditions and/or service level information for the specific service, or services required.

2 Who we are

Panlogic provides public, private and hybrid cloud hosting, support and implementation. We are a Public Sector and Public Sector Solution Provider partner helping the public sector embrace the cloud as part of their digital transformation strategies and deploy Digital First public services in line with Government strategy.

Our teams of certified Solution Architects, DevOps Engineers, SysOps Administrators, Certified Developers and Cloud Practitioners work with customers to find the optimum balance of availability, security and affordability for AWS, Azure and other cloud hosted applications.

Our expertise in AWS and Azure and other cloud hosting, along with associated pricing and service models underpins our ability to make recommendations ranging from strategic advice to tactical delivery that both improve performance and improve efficiency whilst saving cost. Whether you are looking to begin your cloud journey or take it to the next level our unrivalled insight and experience will help you innovate and evolve cloud hosting delivery and support.

3 Portfolio

Our portfolio of Cloud Security services includes:

- Security Strategy and Risk Management
- Secure Architecture and Design
- Security Incident Management and Response
- Security Audit, QA, and Testing Services
- Generalised cloud security consultancy and support services

4 Service definitions

Panlogic provides comprehensive cloud security services, ensuring robust protection for your cloud environments. Our structured approach covers the entire security lifecycle, from developing a tailored security strategy and implementing effective risk management to designing secure architectures and managing security incidents. We also offer thorough security audit services, quality assurance, and testing to guarantee compliance and resilience, providing complete confidence in your cloud operations.

4.1 Security Strategy Development

- We work with you to develop a comprehensive security strategy tailored to your organisation's needs. This involves understanding your business objectives, risk appetite, and compliance requirements to create a robust security framework that aligns with your cloud adoption journey. Our goal is to establish a clear roadmap for achieving and maintaining a strong security posture.

4.2 Security Risk Management

- Our approach to risk management is proactive. We help you identify, assess, and mitigate security risks across your cloud environments. This includes conducting thorough risk assessments, defining risk treatment plans, and implementing controls to reduce your attack surface and protect against potential threats, ensuring business continuity and resilience.

4.3 Security Design

- We integrate security into the core of your cloud architecture. Our experts design secure, resilient, and scalable cloud solutions from the ground up. By applying security-by-design principles, we ensure that your infrastructure and applications are built to withstand threats, protecting data and services while enabling innovation and agility.

4.4 Security Incident Management

- In the event of a security breach, our incident management services provide rapid response and resolution. We establish clear procedures for detecting, containing, and eradicating threats, as well as for recovery and post-incident analysis. Our aim is to minimise the impact of security incidents and reduce downtime.

4.5 Security Audit Services

- We offer comprehensive security audit services to assess your compliance with industry standards and regulatory requirements (e.g., ISO 27001, Cyber Essentials). Our audits identify vulnerabilities and areas for improvement, providing you with actionable recommendations to enhance your security posture and demonstrate due diligence to stakeholders.

4.6 Security Quality Assurance (QA) and Testing

- Our security QA and testing services ensure the effectiveness of your security controls. We conduct rigorous testing, including penetration testing and vulnerability scanning, to identify and remediate weaknesses before they can be exploited. This provides assurance that your systems are secure and perform as expected.

4.7 Service Features

Our cloud security service includes the following key features:

- **Security Strategy Development:** Tailored plans for robust cloud protection.
- **Risk Management:** Proactive identification and mitigation of threats.
- **Security Design:** Architecting secure and resilient cloud solutions.
- **Incident Management:** Rapid response and resolution for security breaches.
- **Security Auditing:** Comprehensive assessments for compliance and vulnerabilities.
- **Quality Assurance:** Rigorous testing to ensure security effectiveness.
- **Compliance Adherence:** Meeting regulatory and industry security standards.
- **Threat Intelligence:** Staying ahead of emerging cyber threats.
- **Data Protection:** Safeguarding sensitive information in the cloud.
- **Continuous Monitoring:** Real-time oversight of cloud security posture.

4.8 Service Benefits

By leveraging Panlogic's cloud security services, you can expect the following benefits:

- **Enhances operational efficiency** through streamlined security processes.
- **Reduces business risk and costs** by preventing security incidents.
- **Accelerates secure innovation** with integrated security from design.
- **Minimises downtime** with swift incident response.
- **Ensures regulatory compliance**, avoiding penalties.
- **Boosts stakeholder confidence** in data integrity.
- **Optimises resource allocation** for security efforts.
- **Strengthens overall security posture** against evolving threats.
- **Improves decision-making** with clear security insights.
- **Fosters a proactive security culture** across the organisation.