IT Security Policy

Design Magic Ltd

Introduction

Design Magic Ltd is a UK-based Managed Services Provider (MSP) and IT consultancy firm serving a diverse global client base. As stewards of sensitive information and critical business operations, Design Magic Ltd is committed to implementing, maintaining, and continually improving a comprehensive IT security policy. This policy ensures alignment with leading security frameworks and certifications, including Cyber Security Essentials and ISO 27001, and supports compliance with applicable laws and regulations.

Purpose

The purpose of this IT Security Policy is to:

- Protect the confidentiality, integrity, and availability of information assets.
- Define roles, responsibilities, and procedures to mitigate risks and respond to security incidents.
- Support compliance with Cyber Security Essentials, ISO/IEC 27001, UK Data Protection Act, GDPR, and other relevant international standards.
- Promote a culture of security awareness and continuous improvement across the organisation.

Scope

This policy applies to all employees, contractors, consultants, and third-party service providers who access, manage, or support Design Magic's information systems, networks, and data, regardless of location or device.

Governance and Responsibilities

- Board of Directors: Ultimate accountability for information security.
- Information Security Manager: Oversees implementation, monitoring, and review of security controls and compliance activities.
- All Employees and Contractors: Must comply with this policy and report any security incidents or concerns.
- IT Department: Responsible for deploying, maintaining, and monitoring technical controls.
- HR Department: Ensures security is embedded in recruitment, onboarding, and training processes.

Compliance with Standards

Design Magic Ltd is committed to full compliance with:

- Cyber Security Essentials (UK)
- ISO/IEC 27001:2013 Information Security Management Systems (ISMS)
- Applicable data protection legislation, including GDPR and the UK Data Protection Act 2018

Regular audits and reviews are conducted to ensure ongoing compliance and certification.

Risk Management

- Systematic identification, assessment, and mitigation of information security risks.
- Maintenance of a Risk Register documenting threats, vulnerabilities, impacts, and mitigation strategies.
- Annual risk assessments, supplemented by ad-hoc reviews in response to significant changes or incidents.
- Security controls are selected based on risk impact and business needs, as specified in ISO 27001 Annex A.

Access Control

- Access to systems and data is strictly controlled on a need-to-know basis.
- Strong authentication practices, including multi-factor authentication for sensitive systems.
- Periodic review and prompt revocation of access rights upon role changes or termination.
- Default “least privilege” policy for all users, accounts, and services.

Asset Management

- All information assets are catalogued and classified according to sensitivity and business criticality.
- Clear ownership and custodianship for all assets.
- Regular inventory reviews and disposal in line with secure destruction procedures.

Physical and Environmental Security

- Secure office locations and data centres with controlled access.
- Protection against environmental threats such as fire, flood, and power disruption.
- Visitor access is restricted and monitored.

Operations Security

- Deployment of firewalls, anti-malware, intrusion detection and prevention systems.
- Vulnerability management through regular patching and updates.
- Secure configuration of all hardware and software.
- Change management processes to ensure secure handling of modifications and upgrades.
- Detailed logging and monitoring of system activities and access.

Communications Security

- Encryption of data in transit and at rest using industry best practices and standards.
- Secure protocols for internal and external communications (e.g., VPN, SSL/TLS).
- Protection of network boundaries and remote connections.

Supplier and Third-Party Management

- Due diligence and compliance checks for all suppliers and partners.
- Mandatory contractual obligations regarding information security and data protection.
- Regular assessments of third-party security controls and performance.

Human Resources Security

- Pre-employment screening, including background checks as appropriate.
- Security awareness training for all staff, with mandatory annual refresher courses.
- Clear disciplinary procedures for breaches of security policy.
- Secure exit procedures to remove access and recover company property.

Information Security Incident Management

- Clear procedures for reporting, investigating, and responding to security incidents.
- Incident Response Team with defined roles and escalation process.
- Post-incident reviews and lessons learned to improve future resilience.
- Maintenance of an incident register, including root cause analysis and corrective actions.

Business Continuity and Disaster Recovery

- Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) reviewed and tested annually.
- Secure, regularly tested backups for all critical systems and data.
- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for key services.

Data Protection and Privacy

- Compliance with GDPR and UK Data Protection Act for all personal data processing.
- Privacy by Design principles embedded in all systems, products, and services.
- Processes for Data Subject Access Requests (DSARs) and data breach notification.

Security Awareness and Training

- Mandatory security induction for new starters.
- Regular communications on emerging threats and best practices.
- Simulated phishing exercises to assess and improve staff vigilance.

Policy Review and Continuous Improvement

- This policy is reviewed annually and after significant changes in business operations or regulatory requirements.
- All staff are encouraged to contribute suggestions to enhance security practices.
- Performance metrics and audit results are used to drive ongoing improvement.

Document Control

- This document is version controlled. Latest version is published on the company intranet.
- Superseded policies are securely archived and accessible for audit purposes.

Conclusion

Design Magic Ltd recognises its responsibility to clients, partners, and stakeholders worldwide to uphold the highest standards of information security. By adhering to this policy, the company seeks to protect its reputation, safeguard its assets, and ensure the ongoing trust of its global clientele.

Last Update: 25th November 2026
Next Review: 25th November 2027