Document ID: TPMG-POL-019
Title: Information Security Statement
Version: 1.0
Status: Approved
Approved by: Giedre Beige - Director

Information Security Statement

1. Purpose

TPMG is committed to protecting the confidentiality, integrity and availability of the information entrusted to us.

This Information Security Statement explains the principles, controls and governance TPMG applies to protect information across its advisory, assurance, audit, training, digital enablement and support activities. It is intended to give clients, suppliers, learners, partners and other stakeholders confidence that information security is treated as a core operational responsibility.

---

2. Scope

This Statement applies to TPMG's handling of information in connection with its business activities, including information relating to clients, prospective clients, website users, suppliers, partners, staff, contractors, learners and other relevant stakeholders.

It applies to information in electronic, physical and verbal form, including where information is processed by authorised third parties on TPMG's behalf.

---

3. Our Commitment

TPMG is committed to maintaining information security through proportionate, risk-based technical and organisational measures.

Our approach is designed to:

- protect information against unauthorised or unlawful access, use, disclosure, alteration, loss or destruction;

- support compliance with applicable UK data protection and privacy requirements;
- reduce avoidable operational, contractual, legal and reputational risk;
- maintain trust with clients, suppliers, staff and stakeholders; and
- promote secure, responsible and consistent ways of working.

This reflects the UK GDPR requirement to process personal data securely using appropriate technical and organisational measures, supported by accountability and review.

---

4. Information Security Principles

TPMG's information security arrangements are based on the following principles:

4.1 Need-to-know access

Access to information is restricted to authorised individuals who require it for legitimate business purposes.

4.2 Least privilege

Access rights are assigned according to role and reviewed when responsibilities change.

4.3 Risk-based protection

Controls are selected and maintained according to the nature of the information, the sensitivity of the processing, and the potential impact of compromise.

4.4 Secure handling by default

Information is expected to be created, stored, shared and disposed of securely as a normal part of delivery.

4.5 Accountability

Security responsibilities are allocated clearly, and compliance is supported by oversight, review and escalation procedures.

These principles are consistent with the example materials you provided, which emphasise risk-based security, classification, legitimate-access controls, secure storage and transfer, incident reporting, training and regular review.

---

5. Governance and Responsibility

TPMG recognises that information security is both a leadership issue and an operational discipline.

- Overall responsibility for information security rests with TPMG leadership.
- Day-to-day security responsibilities are assigned to appropriate internal personnel and, where relevant, trusted specialist providers.
- The Data Protection Officer can be contacted at **dpo@tpmg-group.com** for data protection and privacy-related matters.
- Security incidents, weaknesses, suspicious activity and concerns are expected to be identified, escalated and addressed promptly.
- Security arrangements are reviewed periodically and updated where needed to reflect changes in risk, service delivery, technology or legal obligations.

Your example materials similarly allocate security responsibility to named individuals or departments, require policies to be disseminated to relevant staff, and call for feedback and review mechanisms.

---

6. Core Security Measures

Without disclosing sensitive operational detail, TPMG applies measures that may

include the following, where appropriate to the service, data and risk involved:

6.1 Access control

User access is managed through role-based permissions and controlled onboarding, review and revocation processes.

6.2 Authentication

Accounts and systems are protected through appropriate authentication controls, including strong passwords and additional safeguards where appropriate.

6.3 Secure configuration and maintenance

Devices, software and systems used for TPMG operations are expected to be configured securely and maintained through appropriate update, patching and support arrangements.

6.4 Malware and threat protection

Suitable anti-malware, security monitoring and related controls are used where appropriate to reduce exposure to common threats.

6.5 Encryption and secure transfer

Information is protected in transit and, where appropriate, at rest through suitable encryption and secure transfer methods.

6.6 Backup and resilience

Appropriate backup, continuity and recovery arrangements are maintained to support resilience and timely restoration where required.

6.7 Physical security

Physical records, workspaces and devices containing sensitive or personal information are protected through proportionate physical safeguards.

6.8 Secure disposal

Information and equipment are disposed of securely when no longer required.

These elements align with the measures reflected in your examples, including encryption, secure transfer, secure storage, virus protection, password controls, backups, maintenance, monitored access and secure disposal.

---

7. People, Awareness and Training

TPMG recognises that information security depends on people as much as technology.

Appropriate personnel are expected to understand their responsibilities in relation to confidentiality, information handling, acceptable use, reporting concerns and protecting data in the course of their work. Training, guidance and awareness measures are used where appropriate to support secure behaviour and reduce avoidable risk.

This reflects the emphasis in your example documents on staff awareness, role-based responsibility, supervision and training for those who process personal data or use systems that store it.

---

8. Remote Working, Mobile Devices and BYOD

Where remote working, off-site access, mobile working or bring-your-own-device arrangements are permitted, TPMG expects appropriate safeguards to be applied.

This may include:

- restricting unnecessary storage of sensitive information on local devices;

- securing access to business systems;
- requiring appropriate authentication and device safeguards;
- applying approval and control arrangements where personal devices are used; and
- ensuring that information remains protected outside traditional office environments.

Your example guidance specifically highlights the increased risks associated with remote working, mobile devices and BYOD, and recommends secure access, encryption, review and clear policy controls.

---

9. Third Parties and Supply Chain Security

TPMG uses a proportionate due diligence approach when appointing third-party providers and processors that may access, host, transmit or otherwise process information on our behalf.

Where relevant, TPMG seeks to ensure that third parties:

- provide sufficient guarantees regarding their security measures;
- are bound by appropriate contractual controls;
- handle data only as authorised;
- apply suitable technical and organisational safeguards; and
- support TPMG in meeting relevant legal and contractual obligations.

This reflects ICO guidance on controller-processor arrangements and the need for contracts and due diligence around processors and sub-processors. It is also consistent with your example materials, which require processor agreements, confidentiality obligations, audit rights, security controls and support for data subject rights and incidents.

---

10. Data Protection and Privacy

TPMG's information security approach supports its wider obligations under applicable data protection and privacy law, including the UK GDPR, the Data Protection Act 2018 and, where relevant, PECR.

This includes support for:

- lawful, fair and transparent processing;
- data minimisation and appropriate retention;
- secure storage, handling and sharing;
- breach detection and escalation;
- privacy by design and risk assessment where appropriate; and
- the protection of individuals' rights.

Your example materials repeatedly frame security as both a legal and operational requirement, tied to privacy notices, lawful processing, DPIAs, breach records, retention control and accountability.

---

11. Incident Reporting and Response

TPMG expects actual or suspected information security incidents to be identified and escalated promptly.

Incidents are assessed, contained, investigated and addressed according to their nature, severity and potential impact. Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, TPMG aims to comply with applicable notification requirements, including notification to the ICO where feasible within 72 hours of becoming aware of the breach, and notification to affected individuals where required.

Your example guidance also highlights the importance of internal breach recognition, prompt escalation, record keeping and notifiable breach response.

---

12. Continuous Improvement

Information security is not treated as a one-off exercise. TPMG expects its security arrangements to be reviewed and improved over time in light of:

- changes in services, systems or working practices;
- new risks or vulnerabilities;
- incidents, near misses or lessons learned;
- supplier or platform changes; and
- changes in legal, contractual or client expectations.

This continuous-improvement mindset is reflected in your examples, which call for regular evaluation of measures, review of policies, audit activity and feedback mechanisms.

---

13. Cyber Security Baselines and Good Practice

TPMG recognises the importance of recognised cyber security baselines and good practice frameworks.

Where appropriate to the service, risk and operating environment, TPMG may align aspects of its approach to recognised standards, assurance frameworks and cyber good practice principles. Cyber Essentials is identified by the NCSC as a minimum cyber security standard designed to help organisations defend against the most common internet-based threats.

No certification claim is made in this Statement unless explicitly confirmed elsewhere on the website or in formal TPMG documentation.

---

14. Contact

Document ID: TPMG-POL-019
Title: Information Security Statement
Version: 1.0
Status: Approved
Approved by: Giedre Beige - Director

Questions about this Statement or about TPMG's approach to information security and data protection may be directed to:

TPMG
A trading style of TPMG Group Ltd
Cardinal Point, Park Road, Rickmansworth, WD3 1RE
Tel: 020 7060 6228
General enquiries:admin@tpmg-group.com
Data Protection Officer:dpo@tpmg-group.com
Website:www.tpmg-group.com

---

15. Disclaimer

This Statement is intended to provide a high-level overview of TPMG's information security approach for external audiences. It does not describe every technical, organisational or contractual control used by TPMG, and TPMG may amend or strengthen its controls from time to time in response to operational, legal, contractual or risk requirements.