Peel Group

Cyber Security Policy

OWNER	LAST UPDATED
Information Technology	**April 2024**

Version No 1

1. **Introduction:**

This Information Security Statement aims to provide a summary of information covering security controls within Peel Group.

This Information Security Statement is reviewed annually.

2. **Security Commitment**

We are committed to maintaining and continually improving information security to meet our responsibilities to our customers, shareholders, and investors and to reduce exposure to cyber-attack or breach, operational loss, or reputational damage.

We are committed to ensuring:

- The confidentiality of customer, shareholder, and investors information.
- The integrity of our information.
- That legal requirements are met.
- That information security and risk awareness training is provided to all staff.
- That breach of information or security, actual or suspected, are recorded, and reported and investigated by Peel Information technology team (IT)and overseen by the Risk and Compliance board.

3. **Information Risk and Cybersecurity Organisation**

The Risk and Compliance board, supported by the Executive leadership team are accountable for identifying, assessing, and managing a broad spectrum of risks and compliance.

The Risk and Compliance board ensure that risks and controls are properly managed by Peel Group, its functions, supported by the IT team on an on-going basis.

4. **Security Awareness**

Peel Group has an ongoing security awareness programme employing various channels to engage staff including, intranet content, e-mails, new employee induction and education by undertaking annual mandatory awareness training for all our people.

Completion of annual mandatory training is monitored and failure to complete training results is formal managed by the People and Culture team.

5. **Peel Group Policy**

Peel employs controls through enforcement of policies, standards, and guidelines covering information security and risk. Each policy document is controlled and maintained by a specific owner and reviewed annually by The Risk and Compliance board.

6. **Peel Group policies include but are not limited to**:

- Defined information security responsibilities for employees, contractors, and 3rd parties.
- Testing to identify missing controls or control deficiencies.
- Acceptable usage policies for all users including email and internet usage.
- Defined criteria for access control, including need to know, least privilege principle, unique ID, password complexity, access approvals, leavers processes, privileged access requests, and remote access controls.

- Software development life cycles for applications including code review and security reviews for web services.
- Change control and disaster recovery / business continuity planning requirements.
- End User Environment policies, covering data processing, storage and retention and remote working.
- Technical configuration and control settings for IT infrastructure, networks, and platforms.
- Physical security.

7. Risk Management

Peel Group report and manage risks across the organisation. Information security frameworks follows recognised best practice standards.

Risk assessments are performed periodically to address changes in the information security.

Peel Group performs risk assessments on a variety of assets within the organisation. These may be physical assets, people, processes, software, and information. For example, regular information security risk assessments are performed on application and infrastructure technologies to:

- Identify, quantify, and manage information security.
- Identify activities and factors that pose security risks.
- Ensure information security issues are managed.
- Provide an enterprise view of information security and plans to develop the information security.
- Assess all information security risks, threats, and vulnerabilities.

8. Access Management Control within Peel Group support controls, including:

- New staters, movers, and leavers controls, incorporating segregation of duties principles to ensure authorised least level of privilege entitlements are maintained for all user activities.
- Privileged access is applied once appropriate justification and authorisation had been given, incorporating validation of activities via the IT service desk logging process.
- Access controls ensure all accounts are reviewed, and maintained or revoked, periodically by the appropriate reviewer.

9. **Application Security**

Technical Security is a line of defence that identifies threats, controls, and testing, including:

- Application security and risk assessments – to ensure risks within Peel Group applications and systems are managed to an acceptable level.
- Defining and testing application system controls relating to information security.
- Input to system build standards and procedures.
- Installation and monitoring of application controls.
- Development of minimum baseline security standards.
- Conduct security testing i.e., application penetration test (which includes vulnerabilities).

10. Network Security

To enable effective management Peel Group utilises various technologies deployed strategically throughout the network.

Peel Group networks and infrastructure security are subject to 24/7 monitoring. Wireless Network Management within our offices are secured using access control and monitoring, authentication, encryption, guarding against rogue wireless access points.

- Internet Service provider router devices are fully managed and configured to detect DDoS attacks and always on DDoS mitigation.
- Intrusion Prevention provide alerts to any suspicious activity or attack.
- Internet Access is permitted for business use only. Access is filtered according to centrally defined rules. Additional management approval is required for any non-standard access and may be subject to additional monitoring.
- Data Loss monitoring is in place to reduce exposure to data loss/leakage risk through technical controls and process as well as user education. It includes processes to detect and automatically protect Restricted and Highly Restricted information. This includes outbound e-mail, file transfers and web uploads.
- Peel Group monitors for data leakage to guard against the risks of theft, accidental loss, or deliberate exposure of confidential information.
- Penetration testing is performed by our own IT team as part of our technology improvement processes at regular intervals. In addition, independent testing by specialist third parties may be commissioned, using advanced techniques and latest industry standards to provide additional assurance. The output of such testing is reviewed by the IT Team and reported to the Risk and Compliance board.

11. Host Security

Workstations, Laptops and Mobile devices have anti-virus software incorporated into default operating builds, set to automatically check files as part of its regular full-time “on access” scanning and obtain updates as they become available.

- Desktops/laptops have a single, pre-installed customised build which limits users’ administrative access.
- Laptops are protected against data leakage from device loss via a centrally managed solution.
- Access to the internal network from outside of the office is restricted to authorised devices controlled by industry standard remote connectivity and multi factor authentication controls.
- Internet access and network connectivity from laptops is routed through the Peel Group Proxy network.
- Provided mobile devices are managed through a Unified Endpoint Management solution (UEM) enforcing policies and controls to limit information exposure.
- Mobile data management capabilities enable data to be securely wiped from lost or stolen devices.
- Server Platforms have measures and controls that are incorporated into server builds; these include:
    - Operations/services run with the minimum privileges required; appropriate file system security is applied.
    - Strong user account and password controls are implemented for all users enforcing length, complexity, history, and lockouts. Automated password control with logging and auditing applied to privileged accounts.

- Additional monitoring capabilities are in place to protect sensitive data.
- Configuration settings are defined based on the 'least privilege' principle.
- Monitoring and reporting of any non-compliance.
- Audit log management.

12. Patch Management

Notifications of vulnerabilities and recommended patch responses are undertaken by:

- Prioritisation for deployment is determined by the Patch Classification, assigned as part of the assessment process using Vulnerability Scoring System.
- All patch deployments are managed following Change Management and Incident Management Processes.
- Appropriate governance is exercised through regular engagement and communication with the global providers in accordance with the established framework.
- Monthly patch compliance status of security and operational patches is measured, reported, and distributed.

13. **Remote Working capabilities**

Additional controls and guidance for staff working remotely include:

- Education on remote working.
- Full disk encryption on laptops.
- Secure mobility clients on laptops for VPN use.
- Provision of managed mobile devices via specialist applications.

14. **Physical Security**

Protective security measures are implemented to prevent unauthorised access to Peel Group facilities, resources, or information. Protective security controls are reviewed on a regular basis. Measures deployed are:

- Physical barriers.
- Access control systems and identity cards.
- Surveillance Video Systems (CCTV)
- Secured data and network cabinets.
- Malware detection and mitigation.
- Network and host intrusion detection and monitoring.
- Assessment of emerging technology threats.
- Monitoring of suspicious system access attempts.
- Cyber threat intelligence and reporting.

15. Cybersecurity incident management.

- Co-ordinate Cybersecurity incidents to ensure that all required tasks are completed.
- Ensure that Cybersecurity incidents are investigated in a timely manner.
- Ensure that the risk associated with an incident is appropriately identified, measured, and controlled.
- Ensure all Cybersecurity incidents are centrally tracked for trend analysis.
    - Transfer of information is secured using appropriate technical or process controls.