Pre-license Information Security Requirements For Brokers Control & Market Makers Licenses

Version 1.0

بورصة مسقط

MSX

Information Security Requirements

These requirements aim to provide organizations with practical actionable advice to secure their information assets. They emphasize comprehensive measures covering various aspects of information security, including governance, risk management, asset protection, awareness, incident response, and technical controls.

Cybersecurity Governance & Risk:

- Implement an ISMS and maintain an up-to-date risk register.

Digital & Information Assets:

- Maintain an inventory of hardware, software, and data.
- Identify critical/sensitive information and prioritize its protection.

Security Awareness & Training:

- Train all employees on cyber security relevant to their roles.

Supply Chain Security:

- List and manage suppliers with access to systems and information.
- Include cyber security requirements in their contracts.
- Verify software/hardware integrity before deployment.

Incident Management:

- Develop and test Incident Management, Response, and Disaster Recovery Plans.
- Implement asset backup and recovery procedures.

Identity & Access Management:

- Apply least privilege and disable unused/default accounts.
- Regularly review special access privileges.
- Implement two-factor authentication for remote access.

Passwords & Authentication:

- Enforce strong, unique passwords and regular changes.
- Change default passwords on all assets.
- Provide tools for strong password creation.

Patching & Malware Protection:

- Implement a patch management procedure for applications and firmware.
- Deploy patches within recommended timescales.
- Use active, up-to-date anti-malware protection.

System & Network Security Configuration:

- Deploy active firewalls/gateways to monitor and block unauthorized traffic.
- Secure wireless communication technologies.
- Conduct regular external and internal vulnerability assessments.
- Remove/disable unnecessary applications, ports, and services.

Security Monitoring:

- Monitor internal networks, boundaries, assets, and services for security incidents.

- Retain event/logs for at least 6 months.
- Implement a removable media usage policy.
- Inform Muscat Stock Exchange in case of cyber-attack affecting the Confidentiality, Integrity and Availability on the connectivity with MSX.

Overall, these requirements offer a framework for organizations to build and maintain a comprehensive information security program.