Supplier policy

Information Security and Data Protection | April 2023

For what comes next
tlt.com

Contents

1 Information Security Management

1.1 Have in place a competent information security person/s, which has responsibility for integrating information security consistently into the supplier's business operations.

1.2 Document its Information Security Management Framework, ensuring that it is proportionate to the work being carried out and is in line with laws, regulations, and industry best practices.

1.3 Regularly measure, review, and document its compliance with its documented Information Security Management Framework. As a minimum, the supplier must promptly and accurately complete the Information Security Questionnaire provided by TLT.

2 User Security

2.1 Ensure that all supplier personnel have access only to the systems they are authorised to use and for all systems that they operate within the scope of their defined roles and responsibilities, and regular access reviews are carried out.

2.2 Ensure that all users are uniquely identified, only have access to the systems they require to carry out their role, and ensure that adequate password management controls are enforced, the below should be implemented as a minimum standard:

2.2.1 password length of at least ten (10) characters consisting of at least one Upper Case, Lower Case, Number and Symbol.

2.2.2 password expiry within the maximum of ninety (90) calendar days.

2.2.3 password not to be identical to the previous ten (10) passwords.

2.2.4 enforce a limit of no more than five (5) consecutive invalid access attempts by a user.

2.2.5 prevent further access to the system by initiating a session lock after a maximum of twenty (20) minutes of inactivity.

2.3 Ensure that all supplier personnel are appropriately security vetted before commencing work, and all personnel must complete (at least annually) information security and data protection training.

3 System Security and Network Monitoring

3.1 Ensure that all systems are kept up to date through regular patching and applying security updates within vendor and industry recommended timescales.

3.2 Deploy appropriate security controls to protect the confidentiality, availability and integrity of the systems and data.

3.2.1 Utilise Multi-Factor Authentication (MFA) for user access.

3.2.2 Denial of Service (DoS) protection.

3.2.3 Data Loss Prevention (DLP).

3.2.4 Firewall(s).

3.2.5 Intrusion Detection / Prevention systems (IDS / IPS).

3.2.6 Anti-Virus on all user devices / servers etc.

3.3 Carry out vulnerability scans on a regular basis using industry standard tools, techniques, and methodologies. The supplier shall provide TLT with a summary of results of the scan upon request.

3.4 Ensure that the supplier network is tested at least annually by an industry-recognised security penetration testing process that covers internal and external-facing components.

3.5 Maintain 12 month of appropriate security logs to allow for incident investigation should an incident occur.

3.6 Ensure that access to the supplier's network is monitored and only authorised devices are allowed through appropriate network access controls.

4 Encryption and Data Security

4.1 Ensure that all TLT data and data relating to TLT is encrypted at rest using appropriate industry standard technologies and methodologies.

4.2 Implement as a minimum an industry standard encryption transmitting or electronically accessing TLT Information via a network (eg Transport Layer Security (TLS 1.2) protocol).

4.3 Ensure that all portable devices (eg laptops, tablets, smartphone, removable storage) that hold or have access to any TLT Information, use an industry standard full disk encryption solution.

5 Physical and Environmental Security

5.1 Implement appropriate and effective physical security control processes and systems at its premises in accordance with Good Industry Practice.

5.2 Ensure that all TLT data/information on hard copies is protected in transit and at rest using appropriate physical controls (eg stored in locked cabinets when not in use).

5.3 Ensure that all TLT data/information on hard copies is securely destroyed when no longer required/requested by TLT and certificates of destruction are provided to TLT.

6 Supply Chain Management

Ensure that any third party required to support the services provided to TLT adhere to or exceed the security controls that the supplier is required to comply, and all such services shall be provided under appropriate contractual agreement.

7 Information Security incidents

7.1 Make all reasonable efforts to notify TLT LLP without any undue delay (but no later than 24 hours) of the supplier becoming aware of an actual or potential information security incident affecting TLT data or information relating to TLT.

7.2 Notification must be sent to InformationSecurity@tlt.com.

7.3 Cooperate fully and provide regular update to TLT throughout the incident, to ensure TLT are aware of the scale of the breach and its impact to TLT.

7.4 The supplier will provide a copy of the incident report to TLT once recovery is complete.

tlt.com/contact

Belfast | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus