PULSANT
SUPPLIER SECURITY STANDARDS

Effective Date: 5 January 2026

Owner: Information Security

These Standards set out the minimum security standards applicable to all suppliers, partners and vendors ("**Suppliers**") who have access to the data, systems, networks or facilities ("**Systems**") of Pulsant Ltd or its group companies ("**Pulsant**") and must be applied in a manner proportionate to risk. These are baseline standards and do not supersede any other document requiring greater security, for example any data protection agreement or other contract you have entered into with Pulsant. Suppliers are responsible for compliance with these Standards by each of its employees, contractors, sub-contractors and agents ("**Personnel**") who are provided with access to Pulsant Systems. Pulsant may update these Standards periodically and will notify Suppliers of any material changes. Failure to comply with these Standards may result in suspension or termination of engagement.

1. Personnel

1.1 Suppliers must perform criminal and employment background checks on all Personnel consistent with local laws and regulations. The level of verification performed must be proportional to risk.

1.2 Suppliers must have a comprehensive security awareness program for all Personnel that encompasses education, training and updates for security policies, procedures and requirements. Training must be provided at time of hiring and repeated at regular intervals thereafter.

1.3 Suppliers must promptly remove access to information systems, networks and applications for Personnel who no longer need them.

2. Policies and Procedures

2.1 Suppliers must publish, maintain and enforce formal written information security policies and procedures that are approved by management and communicated to Personnel. Information security policies and procedures must be reviewed regularly and updated as necessary.

3. Verification

3.1 Pulsant may perform security assessments to verify compliance with these Standards. Pulsant will provide reasonable notification of a verification audit and ensure the audit is performed during normal business hours with minimal disruption to business operations.

4. Incident Management

4.1 Suppliers must have documented procedures enabling effective and orderly management of security incidents by trained Personnel covering reporting, analysis, monitoring and resolution.

4.2 Suppliers must report security incidents affecting Pulsant Systems to Pulsant within 72 hours.

4.3 Suppliers must have in place appropriate customer support processes including in relation to vulnerability management, patches and upgrades.

5. IT Security

5.1 Security Controls

5.1.1 Suppliers must perform regular security assessments, scans and testing of information systems, networks and applications.

5.1.2 Suppliers must maintain documented change management procedures for controlling and identifying configuration changes to information systems, networks and applications.

5.2 Network Security

5.2.1 Suppliers must implement and maintain network security infrastructure components such as firewalls, intrusion detection/prevention systems and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks.

5.2.2 Remote access into Suppliers' networks must be approved and restricted to authorised Personnel only. Remote access must be controlled by secure access control protocols, encryption, authentication and logging.

5.2.3 Suppliers may only connect to a Pulsant network, device or service via technical configuration and network architecture agreed with Pulsant. All information about networks, access and security precautions must be treated as confidential.

5.3 Logging

5.3.1 Suppliers must maintain logs from information systems, network devices and applications for a minimum period of 90 days. Logs must provide sufficient details to assist in the identification of the source of an issue and enable a sequence of events to be recreated.

5.4 Malicious Code

5.4.1 Suppliers must use up to date anti-virus/malware detection software to prevent, detect and remove malicious code.

5.4.2 Automatic virus and malware scanning checks must be carried out on all email attachments sent to or received from external sources. Attachments identified as containing malicious code must be removed and deleted.

5.5 Access Controls

5.5.1 Access controls must be implemented for information systems, networks and applications that verify the identity of all users and restrict access to authorised users.

5.5.2 Access lists for information systems, network devices and applications must be reviewed regularly and access removed promptly when no longer required.

5.6 Password Management

5.6.1 Strong password practices must be implemented, including minimum password length and complexity requirements.

6. Back-up, Business Continuity and Disaster Recovery

6.1 Information Backup

6.1.1 Suppliers must ensure information systems, devices and software are backed up to online and/or offline storage.

6.2 Business Continuity and Disaster Recovery

6.2.1 Suppliers must have a documented Disaster Recovery Program and Business Continuity Plan designed to prevent loss of data and ensure continued operation during disruption.

6.2.2 Suppliers must test the Disaster Recovery Program and Business Continuity Plan regularly and will provide confirmation of tests performed, including identified gaps and remediation.

7. Physical Security

7.1 Supplier facilities

7.1.1 Suppliers must maintain a physical security plan that addresses internal and external threats to sites.

7.1.2 Sites must have secure entry points that restrict access and protect against unauthorised access. Access to sites must be limited to authorised Personnel and approved visitors.

7.1.3 Off-site removal of information systems, servers and network devices must be approved by authorised Personnel.

7.2 Pulsant facilities

7.2.1 Supplier Personnel must abide by Pulsant's security requirements and directions when accessing Pulsant facilities. Security measures employed at Pulsant facilities are Pulsant confidential information. Personnel may not photograph or otherwise record Pulsant facilities or infrastructure, unless approved by Pulsant.

7.2.2 Supplier Personnel may not access Pulsant devices, systems or networks unless expressly authorised by Pulsant Personnel.

8. Data Protection

8.1 Suppliers must protect all personal information in accordance with applicable data protection laws (including UK GDPR and the Data Protection Act 2018). Personal information must only be processed for agreed purposes and securely stored, transmitted and deleted when no longer required.

9. Subcontractors

9.1 Suppliers may not engage subcontractors with access to Pulsant Systems without Pulsant's prior written approval. Suppliers remain fully responsible for the acts and omissions of any subcontractors and must ensure they are subject to equivalent security obligations.