Power Integrations Supplier Cybersecurity Policy

Revised Date: JAN2026

The online version of this manual is the updated version and takes precedence over any printed copy

1. Purpose & Scope

This policy establishes the minimum cybersecurity requirements for all Suppliers who handle Power Integrations Confidential Data (PICD) or connect to Power Integrations systems. These requirements ensure business continuity and protect proprietary information across the Power Integrations supply chain.

2. Breach Notification Requirements

Supplier must notify Power Integrations of any Security Incident that impacts or may impact PICD or Power Integrations systems as soon as possible, and no later than **72 hours** after discovery.

- **Initial Notice (within 24 hours):** Preliminary facts and containment actions.
- **Detailed Update (within 72 hours):** Scope, impacted systems, likely impact, and next steps.
- **Required Information:** Date/time of discovery, incident type, status of PICD involvement (confirmed/suspected), and primary incident contact details.

3. Data Encryption & Management

Suppliers must maintain a documented Encryption & Key Management Policy. PICD must be protected using strong, modern cryptographic algorithms:

- **In Transit:** TLS 1.2 or 1.3 for all services, APIs, and secure file transfers (SFTP/FTPS/HTTPS).
- **At Rest:** AES-256 (or equivalent) for storage and backups containing PICD.
- **Key Management:** Access to cryptographic keys must be restricted, logged, and rotated according to policy.

4. Minimum Security Baseline Requirements

Suppliers must implement industry-leading administrative, physical, and technical safeguards.

- **Identity and Access Control:** Enforce the principle of "least privilege". Multi-factor authentication (MFA) is required for all privileged, remote, and internet-facing access to systems handling PICD.
- **Vulnerability & Patch Management:** Maintain routine vulnerability scanning (quarterly recommended). Remediate critical-risk findings within 72 hours for internet-exposed systems.
- **Logging and Monitoring:** Maintain security logs for a minimum of 90 days to enable investigations and audits.
- **Endpoint Protection:** Deploy anti-malware and Endpoint Detection and Response (EDR) controls on all systems accessing PICD.
- **AI/GenAI Restrictions:** Suppliers may not use PICD to train AI/ML models or upload PICD into public AI tools without prior written approval from Power Integrations.

- **Subcontractor Accountability:** Suppliers remain accountable for compliance when engaging subcontractors; PICD access must not be provided to third parties without prior notification and approval.

5. Supplier Acknowledgement & Attestation

The Supplier confirms receipt and understanding of this policy and attests that the required controls are implemented.

A. **Compliance Attestation**

- [ ] Documented Incident Response Plan in place.
- [ ] 72-hour breach notification window accepted.
- [ ] Encryption standards (AES-256/TLS 1.2+) met.
- [ ] MFA and least-privilege access enforced.
- [ ] Vulnerability scanning and timely patching implemented.
- [ ] Security logs retained for investigations.

Power Integrations Incident Reporting Contact: Breach-notify@power.com