

POWERUS CORPORATION

GOVERNMENT DATA PROTECTION POLICY

(A Nevada Corporation, Nasdaq: PUSA)

Adopted: October 1, 2026
Approved by the Board of Directors

1. PURPOSE

This Government Data Protection Policy (this “Policy”) of Powerus Corporation, a Nevada corporation (Nasdaq: PUSA) (the “Company”), and its consolidated subsidiaries (together with the Company, the “Powerus Group”) establishes the requirements for identifying, marking, safeguarding, transmitting, storing, reporting on, and disposing of Government Data. It supplements the Company’s Confidential Information Policy, under which Government Data is a category of Confidential Information, and controls over that policy to the extent this Policy imposes more restrictive requirements.

The Powerus Group performs U.S. government contracts and subcontracts involving Controlled Unclassified Information, Federal Contract Information, classified programs, and export-controlled technical data. Mishandling Government Data can result in loss of contract eligibility, civil and criminal liability, suspension or debarment, and loss of the Company’s facility security clearance.

This Policy is designed to implement, among other applicable authorities:

- i. Executive Order 13556 and 32 C.F.R. Part 2002 (Controlled Unclassified Information), and the CUI Registry maintained by the National Archives and Records Administration;
- ii. DoD Instruction 5200.48 (Controlled Unclassified Information);
- iii. DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) and NIST SP 800-171;
- iv. DFARS 252.204-7019 and 252.204-7020 (NIST SP 800-171 DoD Assessment and SPRS) and DFARS 252.204-7021 and 252.204-7025 (Cybersecurity Maturity Model Certification);
- v. FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems) with respect to Federal Contract Information;
- vi. Executive Order 13526 and the National Industrial Security Program Operating Manual, 32 C.F.R. Part 117 (NISPOM), for Classified Information; and
- vii. the International Traffic in Arms Regulations and the Export Administration Regulations, as further addressed in the Company’s Export Control and ITAR Compliance Policy.

2. **SCOPE**

This Policy applies to all directors, officers, employees, contractors, subcontractors, suppliers, consultants, advisors, and agents of the Powerus Group who access, receive, create, or otherwise handle Government Data (collectively, “Covered Persons”), and applies in addition to the Confidential Information Policy and any confidentiality obligations in a Covered Person’s engagement agreement. Obligations under this Policy survive the termination of employment or engagement.

3. **DEFINITIONS**

a. **“Government Data”** means CUI, Federal Contract Information, Covered Defense Information, Classified Information, and any other non-public information that the Powerus Group receives from, generates for, or handles on behalf of the U.S. government or a higher-tier government contractor.

b. **“Controlled Unclassified Information”** or “CUI” has the meaning set forth in 32 C.F.R. Part 2002 and the CUI Registry: information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

c. **“Covered Defense Information”** or “CDI” means unclassified controlled technical information or other information, as described in the CUI Registry, that requires safeguarding or dissemination controls and is collected, developed, received, transmitted, used, or stored in support of the performance of a contract subject to DFARS 252.204-7012.

d. **“Federal Contract Information”** or “FCI” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service, as defined in FAR 52.204-21.

e. **“Classified Information”** means information determined pursuant to Executive Order 13526, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and designated at the Confidential, Secret, or Top Secret level, including Sensitive Compartmented Information and Special Access Program information.

f. **“Covered Contractor Information System”** means an information system that is owned or operated by or for the Powerus Group and that processes, stores, or transmits CUI or CDI.

g. **“Need to Know”** means a determination that a proposed recipient requires access to specific Government Data to perform assigned duties, and does not authorize access above the level and scope covered by the recipient’s personnel security clearance.

h. **Other Terms.** Capitalized terms not defined in this Policy have the meanings given in the Confidential Information Policy.

4. **ROLES AND RESPONSIBILITIES**

a. **General Counsel.** Administers this Policy, makes legal determinations regarding Government Data, and directs the Company's response to incidents and disclosure demands.

b. **Facility Security Officer.** The Facility Security Officer ("FSO") administers the Company's classified access program and NISPOM compliance.

c. **Insider Threat Program Senior Official.** The Insider Threat Program Senior Official ("ITPSO") administers the Company's Insider Threat Program under 32 C.F.R. § 117.7.

d. **IT Security.** Implements and monitors technical safeguards, maintains the System Security Plan, and leads incident response for Covered Contractor Information Systems.

e. **Covered Persons.** Comply with this Policy, complete required training, and report incidents and insider-threat indicators promptly.

5. **IDENTIFICATION, MARKING, AND DISSEMINATION OF CUI**

a. **Marking.** CUI must be identified and marked in accordance with 32 C.F.R. § 2002.20 and DoD Instruction 5200.48, including the CUI banner marking, applicable category markings, and any Limited Dissemination Controls.

b. **Legacy Markings.** Legacy "FOUO," "SBU," and similar markings do not by themselves establish CUI status; information bearing such markings must be re-evaluated and, where appropriate, re-marked as CUI.

c. **Dissemination.** CUI may be shared only with recipients who have a lawful Government purpose and a Need to Know, subject to any Limited Dissemination Controls.

d. **Decontrol.** CUI may be decontrolled only by or at the direction of the designating agency or as authorized by the CUI Registry. Covered Persons may not unilaterally remove CUI markings.

6. **SAFEGUARDING REQUIREMENTS**

a. **NIST SP 800-171.** Each Covered Contractor Information System must implement the security requirements of NIST SP 800-171 at the revision required by the applicable contract. Although NIST published Revision 3 on May 14, 2024, DoD contracts and CMMC Level 2 assessments remain measured against Revision 2 under DoD Class Deviation 2024-O0013 until that deviation is rescinded, so Covered Persons must implement the revision specified in the applicable contract.

b. **System Security Plan.** The Company must maintain a current System Security Plan and Plan of Action and Milestones for each Covered Contractor Information System.

c. **Encryption.** CUI and CDI must be encrypted at rest and in transit using FIPS 140-validated cryptographic modules.

d. **Cloud Services.** CUI and CDI may be stored or processed in a cloud service only where the service provider meets the FedRAMP Moderate (or equivalent) baseline and complies with the requirements of DFARS 252.204-7012(b)(2)(ii)(D).

e. **Access and Media.** Access must be limited to authorized users with a Need to Know. Removable media and mobile devices holding Government Data must be encrypted, inventoried, and controlled, and Government Data may not be stored on personal devices or unauthorized services.

7. **SPRS ASSESSMENT AND CMMC**

a. **SPRS.** The Company must conduct and maintain a current NIST SP 800-171 DoD Assessment and post the resulting score in the Supplier Performance Risk System (SPRS) as required by DFARS 252.204-7019 and 252.204-7020.

b. **CMMC.** The Company must hold the Cybersecurity Maturity Model Certification level required by each applicable contract under DFARS 252.204-7021 and 252.204-7025. CMMC requirements began phasing into DoD solicitations and contracts on November 10, 2025 under a three-year rollout, and the Company must submit the required annual affirmation of continuing compliance in SPRS.

8. **CYBER INCIDENT REPORTING AND CUI SPILLAGE**

a. **Seventy-Two Hour Reporting.** Any cyber incident affecting a Covered Contractor Information System or the CDI residing on it must be reported to the U.S. Department of Defense through the DIBNet portal within seventy-two (72) hours of discovery, using the Company's DoD-approved medium assurance certificate, in accordance with DFARS 252.204-7012(c).

b. **Preservation and Malware.** The Company must preserve and protect images of affected systems and relevant monitoring data for at least ninety (90) days from the incident report, provide access to the Government upon request, and submit any malicious software isolated in connection with the incident.

c. **Internal Notification.** Covered Persons must report any suspected incident to IT Security, the FSO, and the General Counsel immediately.

d. **CUI Spillage.** Suspected spillage of CUI onto an unauthorized system that does not constitute a reportable cyber incident must be reported to the FSO and the General Counsel immediately and handled through the Company's incident-response procedures, including containment, sanitization, and notification of the designating agency where required.

9. **CLASSIFIED INFORMATION AND INSIDER THREAT**

a. **Supremacy of Government Requirements.** Classified Information is governed by the applicable security classification guides, program security instructions, DD Form 254, government security agreements, and the NISPOM (32 C.F.R. Part 117), which control over this Policy in the event of any conflict.

b. Access. Access to Classified Information requires a current personnel security clearance at the appropriate level and a documented Need to Know. No Covered Person may access Classified Information above their granted clearance. The FSO administers the classified access program.

c. Handling. Classified Information must be stored, processed, and transmitted only in approved facilities and systems, must not be removed from an approved location without proper authorization, and must never be placed on a personal system.

d. Insider Threat Program. The Company maintains an Insider Threat Program under 32 C.F.R. § 117.7. Covered Persons must report insider-threat indicators and potential compromises of Government Data to the ITPSO and the FSO.

10. TRANSMISSION AND EXTERNAL RELEASE

a. Screening Before Transmission. Before transmitting Government Data to any recipient, the sending Covered Person must confirm that the recipient is authorized for that data and destination and that the transmission uses an approved, encrypted system or approved physical means.

b. Foreign Persons. Disclosure of export-controlled technical data to a foreign person, including a foreign-person employee within the United States, is a deemed export requiring prior Legal Department clearance under the Export Control and ITAR Compliance Policy (22 C.F.R. § 120.17; 15 C.F.R. §§ 734.13 and 734.20).

c. Public Release. Government Data may not be publicly released. Technical data intended for public release must undergo Legal Department pre-publication review before release.

11. SUBCONTRACTOR AND SUPPLIER FLOWDOWN

Covered Persons responsible for procurement must flow down the safeguarding, cyber-incident-reporting, and certification requirements of DFARS 252.204-7012(m) and 252.204-7021, and the FAR 52.204-21 safeguarding requirements for FCI, to subcontractors and suppliers that will process, store, or transmit Government Data, and must verify each such subcontractor's or supplier's SPRS and CMMC status before award.

12. CHANGE OF CONTROL, NOVATION, AND FOCI

In connection with any change of control, merger, acquisition, or novation involving the Company, Government Data may not be disclosed to acquiring or merging parties without prior authorization from the applicable Government contracting authority and, for Classified Information, approval from the Defense Counterintelligence and Security Agency ("DCSA"). The General Counsel and FSO must be consulted immediately upon any contemplated transaction that may affect the Company's facility security clearance or trigger foreign ownership, control, or influence ("FOCI") mitigation.

13. RETENTION, RETURN, AND DESTRUCTION

a. **CUI.** Destruction of CUI must meet the media-sanitization standards of NIST SP 800-88 and 32 C.F.R. § 2002.14.

b. **Classified Information.** Classified Information must be retained, returned, or destroyed solely through the FSO and applicable Government procedures and must never be retained on any personal system.

c. **Contract Requirements.** Government Data must otherwise be retained or returned as required by the applicable contract and the Company's Document Retention Policy.

14. **TRAINING AND ACKNOWLEDGMENT**

Covered Persons who handle Government Data must complete required CUI, security, and insider-threat training before receiving access and at least annually thereafter, and must acknowledge this Policy in writing. The General Counsel and FSO maintain records of training and acknowledgment.

15. **REPORTING AND NON-RETALIATION**

Covered Persons must report suspected violations of this Policy, unauthorized disclosures, and incidents to the General Counsel, and to the FSO and ITPSO as applicable. The Company will not retaliate against any Covered Person for making a good-faith report. Nothing in this Policy limits any reporting rights preserved under the Confidential Information Policy or the SEC whistleblower rules.

16. **RELATIONSHIP TO OTHER POLICIES**

This Policy supplements and must be read together with the Confidential Information Policy, the Export Control and ITAR Compliance Policy, the Information Security Policy, the Insider Threat Program, and the Document Retention Policy. In the event of any conflict, the more specific and more restrictive requirement governs.

17. **ADMINISTRATION AND REVIEW**

The General Counsel is responsible for administering this Policy, distributing it to Covered Persons, responding to questions, and maintaining records of acknowledgment. The General Counsel will present this Policy to the Audit Committee of the Board of Directors for review at least annually. The Company reserves the right to amend or rescind this Policy at any time.

* * *

Acknowledgment Form Follows

POWERUS CORPORATION
GOVERNMENT DATA PROTECTION POLICY
ACKNOWLEDGMENT FORM

I, the undersigned, acknowledge and certify that:

- (1) I have received and read the Powerus Corporation Government Data Protection Policy (the “Policy”).
- (2) I understand my obligations to identify, mark, safeguard, transmit, store, report on, and dispose of Government Data, including CUI and Classified Information, in accordance with the Policy and applicable law.
- (3) I understand that Government Data must be handled only on authorized systems and disclosed only to persons with proper authorization and a Need to Know.
- (4) I agree to report any suspected incident, spillage, or insider-threat indicator immediately as required by the Policy.
- (5) I understand that violations of the Policy may result in disciplinary action, up to and including termination for cause, as well as civil and criminal liability.
- (6) I understand that my obligations under the Policy survive the termination of my employment or engagement with the Powerus Group.

Signature

Title / Department

Print Name Legibly

Date