

POWERUS CORPORATION
CONFIDENTIAL INFORMATION POLICY

(A Nevada Corporation — Nasdaq: PUSA)

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

1. PURPOSE

This Confidential Information Policy (this “Policy”) of Powerus Corporation, a Nevada corporation (Nasdaq: PUSA) (the “Company”), and its consolidated subsidiaries (each a “Subsidiary” and collectively the “Subsidiaries,” and together with the Company, the “Powerus Group”), establishes the rules governing the identification, handling, protection, use, and disclosure of Confidential Information.

The Powerus Group develops, manufactures, and supports advanced autonomous systems, unmanned aerial vehicles, and related defense technologies. Its operations involve government contracts, classified programs, export-controlled technical data, and sensitive intellectual property. Protecting Confidential Information is essential to the Company’s competitive position, its legal and regulatory compliance, its government contracting eligibility, and the trust of its customers, partners, and investors.

This Policy is designed to ensure compliance with, among other applicable laws and regulations:

- i. The Nevada Uniform Trade Secrets Act, NRS Chapter 600A;
- ii. The federal Defense Trade Secrets Act of 2016 (“DTSA”), 18 U.S.C. §§ 1836–1839;
- iii. The International Traffic in Arms Regulations (“ITAR”), 22 C.F.R. Parts 120–130;
- iv. The Export Administration Regulations (“EAR”), 15 C.F.R. Parts 730–774;
- v. The National Industrial Security Program Operating Manual (“NISPOM”), 32 C.F.R. Part 117, and applicable government security agreements for classified programs;
- vi. DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) and related Cybersecurity Maturity Model Certification (“CMMC”) requirements;
- vii. FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems);
- viii. Regulation FD and the Company’s Insider Trading and Communications Policy with respect to material nonpublic information;
- ix. The SEC whistleblower protection rules promulgated under the Dodd-Frank Wall Street Reform and Consumer Protection Act; and

- x. Applicable state and federal data privacy and security laws.

2. **SCOPE — PERSONS COVERED**

This Policy applies to all directors, officers, employees (full-time, part-time, and temporary), contractors, subcontractors, suppliers, consultants, advisors, and agents of the Company and any Subsidiary who access, receive, create, or otherwise handle Confidential Information in the course of their engagement with the Powerus Group (collectively, “Covered Persons”). Covered Persons who are contractors, subcontractors, suppliers, consultants, or advisors are bound by this Policy in addition to any confidentiality obligations in their engagement agreements.

Obligations under this Policy survive the termination of employment or engagement with the Powerus Group, as set forth in Section 11.

3. **DEFINITIONS**

a. “***Confidential Information***” means all non-public information, in any form or medium (oral, written, electronic, or otherwise), whether so designated or not, that relates to the business, operations, technology, customers, personnel, financial condition, or strategic plans of the Powerus Group or of any third party whose information is entrusted to the Powerus Group, including without limitation:

- i. Trade Secrets (as defined below);
- ii. Business Information: financial data, projections, budgets, pricing, cost structures, customer lists, vendor relationships, contracts, business strategies, acquisition plans, personnel information, and compensation data;
- iii. Technical Information: software code, algorithms, firmware, system architectures, engineering designs, product specifications, test data, research and development materials, manufacturing processes, and other technical data relating to the Company’s autonomous systems, unmanned aerial vehicles, energy systems, and related technologies;
- iv. Government Information: information received from, generated under, or associated with U.S. government contracts, including Controlled Unclassified Information (“CUI”), Classified Information (as defined below), For Official Use Only (“FOUO”) information, and any other information designated or marked as sensitive under applicable government marking schemes;
- v. Export-Controlled Information: technical data, technology, software, and other information subject to ITAR, EAR, or other applicable export control laws;
- vi. Personal Data: information relating to identified or identifiable natural persons, including employee records, benefits information, and customer personal information;
- vii. Third-Party Confidential Information: information received from customers, suppliers, partners, investors, or other third parties subject to a duty of confidentiality or a non-disclosure agreement; and

viii. **Material Nonpublic Information (“MNPI”)**: information about the Company or its securities that is both material and nonpublic, as defined in the Company’s Insider Trading and Communications Policy.

b. **“Trade Secrets”** means information, including technical and non-technical data, formulas, patterns, compilations, programs, devices, methods, techniques, and processes, that derive independent economic value from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from their disclosure or use, and are subject to reasonable measures to maintain their secrecy, as protected under NRS Chapter 600A and the Defend Trade Secrets Act.

c. **“Classified Information”** means information that has been determined pursuant to Executive Order 13526, or any predecessor or successor order, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure, and that is so designated with a classification level (e.g., Confidential, Secret, or Top Secret), including Sensitive Compartmented Information (“SCI”) and Special Access Program (“SAP”) information.

d. **“Controlled Unclassified Information” or “CUI”** has the meaning set forth in 32 C.F.R. Part 2002 and the CUI Registry maintained by the National Archives and Records Administration, and includes 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.

e. **“Need to Know”** means, for purposes of this Policy, a determination by an authorized holder of Confidential Information that a proposed recipient requires access to specific Confidential Information in order to perform their assigned duties, and does not constitute authorization for access to Classified Information above the level and scope covered by the recipient’s personnel security clearance.

f. **“Permitted Disclosure”** has the meaning set forth in Section 6.

4. **OBLIGATIONS OF COVERED PERSONS**

a. **Duty of Confidentiality.** Each Covered Person has a duty to protect all Confidential Information to which they have access in the course of their engagement with the Powerus Group. Covered Persons must:

i. Use Confidential Information solely for the legitimate business purposes of the Powerus Group;

ii. Not disclose Confidential Information to any person outside the Powerus Group except as expressly authorized by Section 6 of this Policy;

iii. Not disclose Confidential Information to other Covered Persons who do not have a Need to Know;

iv. Take all reasonable steps to prevent the unauthorized access to, disclosure of, or use of Confidential Information;

v. Immediately report any known or suspected unauthorized access to or disclosure of Confidential Information to the General Counsel in accordance with Section 12; and

vi. Upon termination of employment or engagement, return or destroy Confidential Information as required by Section 11.

b. *No Personal Use.* Covered Persons may not use Confidential Information for personal gain or for the benefit of any third party, including any competitor, prospective employer, or investment account. Trading in Company Securities while in possession of MNPI is prohibited by the Insider Trading and Communications Policy and applicable federal securities laws.

c. *No Solicitation of Third-Party Confidential Information.* Covered Persons must not solicit, accept, or use confidential information belonging to a third party (including a former employer of any Covered Person) if doing so would violate any obligation owed to that third party. Covered Persons who believe they may possess confidential information belonging to a former employer should notify the General Counsel before using or relying on any such information.

d. *Duty to Disclose Company-Related Innovations.* Covered Persons who create, develop, or conceive of any invention, discovery, design, development, improvement, process, software, work of authorship, or other intellectual property in the course of their engagement with the Powerus Group must promptly disclose such development to their supervisor and to the Legal Department in accordance with any applicable Invention Assignment Agreement.

e. *Ongoing Nature of Obligation.* The duty of confidentiality is a continuing obligation that applies at all times during and after a Covered Person's engagement with the Powerus Group. The passage of time does not diminish the obligation with respect to information that remains non-public and continues to qualify as Confidential Information.

5. INFORMATION CATEGORIES AND HANDLING STANDARDS

The Powerus Group uses the following information classification categories. All Confidential Information must be handled in accordance with the most restrictive standard applicable to its classification.

Category	Examples	Handling Standard	Disclosure
RESTRICTED — CLASSIFIED	TS/SCI, Secret, Confidential national security information	NISPOM / government security agreement controls; access limited to cleared personnel with Need to Know	Only as authorized by applicable government security authority; see Section 7

RESTRICTED — EXPORT CONTROLLED	ITAR technical data; EAR controlled technology; USML items	No disclosure to foreign persons without license or exception; encrypted transmission; access controls	Only with required export authorization; see Section 8
RESTRICTED — CUI	Controlled Unclassified Information; FOUO; law enforcement sensitive	Per applicable CUI category requirements (32 C.F.R. Part 2002); need- to-know access; DFARS 252.204-7012	Government and contractor personnel with Need to Know and authorized access only
CONFIDENTIAL — PROPRIETARY	Trade secrets; IP; M&A plans; financial models; unpublished products	Password-protected; encrypted at rest and in transit; labeled; access controls; no storage on personal devices	Internal Need to Know; external only under signed NDA or Permitted Disclosure
CONFIDENTIAL — BUSINESS	Pricing; customer lists; personnel data; strategic plans; MNPI	Access controls; not shared externally without authorization; MNPI treated per Insider Trading Policy	Internal Need to Know; external under NDA or as required by law
INTERNAL USE ONLY	Internal policies; org charts; general operational information	Not for public distribution; standard access controls	Internal only unless authorized

Where information does not bear a classification marking, Covered Persons should assess its sensitivity in light of this Policy and handle it in accordance with the most appropriate category. When in doubt, treat information as Confidential — Proprietary and consult the General Counsel.

6. **PERMITTED DISCLOSURES**

a. *Internal Disclosures.* Covered Persons may share Confidential Information within the Powerus Group with other Covered Persons who have a legitimate Need to Know in connection with their assigned responsibilities. The fact that a recipient is an employee does not itself establish a Need to Know.

b. *External Disclosures Under NDA.* Confidential Information may be disclosed to third parties — including customers, vendors, partners, investors, financing sources, and professional advisors — only:

i. Pursuant to a written non-disclosure or confidentiality agreement approved by the Legal Department that adequately restricts the use and further disclosure of the information; or

ii. Pursuant to a contract that expressly governs the disclosure and includes appropriate confidentiality protections.

c. *Legal and Regulatory Disclosures.* Confidential Information may be disclosed without prior authorization:

i. To legal counsel (inside or outside) of the Powerus Group, subject to the attorney-client privilege;

ii. As required by applicable law, legal process, court order, or binding regulatory requirement — provided that, to the extent permitted by law, the Covered Person first notifies the General Counsel and cooperates with the Company's efforts to seek a protective order or other appropriate protection;

iii. To the SEC, CFTC, DOJ, EEOC, NLRB, or any other federal or state regulatory authority or law enforcement agency, in connection with a good-faith report of a potential legal violation. Nothing in this Policy limits any Covered Person's rights or obligations under the SEC's whistleblower program (17 C.F.R. §§ 240.21F-1 through 240.21F-17) or any other federal or state whistleblower protection statute. No prior authorization from the Company is required for such reports, and the Company will not retaliate against any Covered Person for making such a report; and

iv. As authorized in writing by the General Counsel or Chief Legal Officer for a specific purpose.

d. *Public Information.* Information that has been intentionally and lawfully made available to the general public by the Company through a press release, SEC filing, or other authorized public communication is not subject to confidentiality restrictions under this Policy. Covered Persons who are unsure whether specific information has been made public should confirm with the Legal Department or Investor Relations before treating it as public. This subsection does not authorize the release of any export-controlled information, CUI, or Classified Information, which remains restricted regardless of whether related information has been made public.

e. *Reg FD and MNPI.* All disclosures of information about the Company to investors, analysts, journalists, or other members of the public are subject to the additional requirements of Regulation FD and the Company's Insider Trading and Communications Policy. Covered Persons who are not authorized spokespersons must not disclose any Company financial or operational information to external parties. Refer all such inquiries to the Legal Department or Investor Relations.

7. GOVERNMENT CONTRACTS AND CLASSIFIED INFORMATION

a. *Supremacy of Government Security Requirements.* With respect to Classified Information and CUI, the requirements of this Policy are supplemented — and in the event of any conflict, superseded — by the applicable government security classification guides, program security instructions, DD Form 254

(Contract Security Classification Specification), NISPOM (32 C.F.R. Part 117), and applicable government security agreements. Covered Persons who work on classified programs must comply with those requirements in addition to this Policy.

b. *Access to Classified Information.* Access to Classified Information requires a current personnel security clearance at the appropriate level granted by the relevant U.S. government agency and a documented Need to Know for the specific classified information sought. No Covered Person may access Classified Information at a level above their granted clearance. The Facility Security Officer (“FSO”) is responsible for administering the Company’s classified access program.

c. *CUI Handling.* All CUI received from or generated in performance of U.S. government contracts must be handled in accordance with 32 C.F.R. Part 2002, NARA’s CUI Registry, applicable CUI category-specific requirements, and DFARS 252.204-7012 (Safeguarding Covered Defense Information). Covered Persons who handle CUI must complete all required CUI training and must report any CUI spillage or unauthorized disclosure to the FSO and the General Counsel immediately.

d. *No Unauthorized Removal.* No Classified Information or CUI may be removed from an approved secure facility or government-designated location without proper authorization. Electronic transmission of Classified Information or CUI must comply with applicable government security requirements and approved communication systems.

e. *Change-of-Control and Novation.* In connection with any change of control, merger, or acquisition involving the Company, Classified Information and CUI 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”) or applicable agency. The General Counsel and FSO must be consulted immediately upon any contemplated transaction that may affect the Company’s facility security clearance.

f. *Government Data Protection Policy.* The detailed requirements for identifying, marking, safeguarding, transmitting, storing, reporting on, and destroying CUI, Classified Information, Federal Contract Information, and other Government Information, including the applicable NIST SP 800-171, DFARS, SPRS, and CMMC obligations, are set forth in the Company’s Government Data Protection Policy, which supplements this Policy and, to the extent it imposes more restrictive requirements, controls.

8. EXPORT-CONTROLLED INFORMATION

a. *Prohibition on Unauthorized Export.* No Covered Person may export, re-export, transfer, or disclose any export-controlled technical data, technology, software, hardware, or other item without first:

- i. Determining, in consultation with the Legal Department, whether an export license, license exception, or other authorization is required;
- ii. Obtaining all required export authorizations; and
- iii. Confirming in writing with the Legal Department that the proposed disclosure or transfer is compliant with applicable ITAR, EAR, and other export control requirements.

b. *Deemed Export Rule.* Covered Persons must be aware that the disclosure of export-controlled technical data to a foreign national — even within the United States — constitutes a deemed export under U.S. law and may require an export license. No export-controlled technical data may be disclosed to a foreign national without prior Legal Department authorization.

c. *Marking and Identification.* Technical data and technology subject to ITAR or EAR controls should be marked or identified as export-controlled to the extent practicable. The absence of a marking does not relieve a Covered Person of the obligation to assess and comply with applicable export control requirements.

d. *ITAR Registration and TAAs.* The Company maintains ITAR registration with the U.S. Department of State Directorate of Defense Trade Controls (“DDTC”). All Technical Assistance Agreements (“TAAs”), Manufacturing License Agreements (“MLAs”), and other ITAR-authorized agreements must be coordinated through the Legal Department before any related disclosure or performance.

e. *Reporting.* Any suspected unauthorized export, deemed export, or disclosure of export-controlled information must be reported immediately to the Legal Department. The Legal Department will assess whether a voluntary self-disclosure to DDTC or BIS is required or appropriate.

f. *Screening Before Transmission.* No Covered Person may transmit, send, forward, upload, ship, or otherwise release any export-controlled technical data, technology, software, or hardware, by any means and to any recipient (whether external or internal to the Powerus Group, and whether in electronic or physical form), until the Covered Person has confirmed that the specific transmission is authorized under an applicable license, license exception or exemption, or other authorization, or that the item is not subject to export control. Disclosure or transfer of 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 (22 C.F.R. § 120.17; 15 C.F.R. §§ 734.13 and 734.20). When in doubt, a Covered Person must treat the item as controlled and obtain clearance before sending.

g. *Pre-Publication Review.* Technical data intended for public release, including papers, conference presentations, marketing materials, and public code repositories, must undergo Legal Department pre-publication review to confirm that it qualifies for the ITAR public-domain exclusion (22 C.F.R. § 120.34) or the EAR published exclusion (15 C.F.R. § 734.7) before release. The absence of a marking does not permit release without review.

9. PERSONAL DATA

a. *Applicable Law.* The collection, use, storage, and disclosure of Personal Data relating to employees, contractors, customers, or other individuals must comply with applicable federal and state data privacy and security laws, including (as applicable) the California Consumer Privacy Act (“CCPA”) as amended by the California Privacy Rights Act (“CPRA”), and any other applicable state privacy laws. Personal Data is Confidential Information subject to this Policy.

b. *Minimization.* Covered Persons must collect and retain only the minimum Personal Data necessary for the legitimate business purpose for which it is collected. Personal Data must not be used for any purpose other than the purpose for which it was collected, unless separately authorized.

c. **Security.** Personal Data must be stored and transmitted using appropriate technical and organizational security measures consistent with the Company's Information Security Policy. Personal Data must not be stored on personal devices, unencrypted portable media, or unauthorized cloud services.

d. **Breach Reporting.** Any known or suspected unauthorized access to, disclosure of, or loss of Personal Data must be reported to the General Counsel immediately. The Company's legal obligations regarding breach notification will be assessed and managed by the Legal Department in coordination with IT Security.

10. **INFORMATION PROTECTION REQUIREMENTS**

a. **Physical Security.** Covered Persons must secure physical documents and media containing Confidential Information when not in use. Documents must be stored in locked cabinets or secure facilities as appropriate to their classification. Confidential documents must be shredded or otherwise securely destroyed when no longer needed, in accordance with the Company's Document Retention Policy.

b. **Electronic Security.** Covered Persons must:

- i. Access Confidential Information only through Company-approved systems and devices;
- ii. Use strong, unique passwords and multi-factor authentication for all systems containing Confidential Information;
- iii. Encrypt Confidential Information when transmitted electronically, using Company-approved encryption methods;
- iv. Not store Confidential Information on personal devices, personal cloud storage accounts, or any systems not approved by the Company's IT Security function;
- v. Not forward, copy, or transfer Confidential Information to personal email accounts; and
- vi. Lock screens and secure devices when leaving them unattended.

c. **Remote Work.** Covered Persons who access Confidential Information while working remotely must comply with the Company's Remote Work and Information Security policies, including using only approved VPN connections and encrypted devices, and ensuring that Confidential Information is not visible or audible to unauthorized persons.

d. **Social Media and Public Platforms.** Covered Persons must not post, share, transmit, or discuss any Confidential Information on social media platforms, online forums, messaging applications, or any other public or semi-public platform. This prohibition applies regardless of whether the platform is accessed on a personal or Company device. See also the Powerus Employee Communications Handbook for additional guidance on public communications.

e. ***Third-Party Visitors.*** Covered Persons must not allow third-party visitors to access any area containing Confidential Information, classified materials, or restricted hardware without prior authorization from the applicable program manager, FSO, or the Legal Department, and must escort all visitors in restricted areas at all times.

f. ***Clean Desk / Clean Screen.*** Covered Persons working in shared or open-plan environments must maintain a clean desk policy — ensuring that Confidential Information is not left visible on desks, screens, whiteboards, or other surfaces when not actively in use.

g. ***Export-Controlled Data.*** Export-controlled data must be encrypted in transit and at rest using FIPS 140-validated cryptographic modules and may be stored or processed in a cloud service only where the service prevents access by unauthorized foreign persons. CUI and other Government Data are subject to the additional cloud, encryption, and safeguarding requirements of the Government Data Protection Policy.

h. ***Screening Before External Transmission.*** Before transmitting any Confidential Information to a recipient outside the Powerus Group, the sending Covered Person must confirm that the information has been screened and cleared for that transmission, including confirmation that it contains no export-controlled data, CUI, or Classified Information that is not authorized for the recipient and destination.

i. ***Generative Artificial Intelligence Tools.*** No Covered Person may input, upload, or paste any Confidential Information, source code, technical data, CUI, export-controlled data, or MNPI into any public or consumer generative artificial-intelligence or large-language-model tool, or any artificial-intelligence service not approved in writing by the IT Security function and the Legal Department. Approved enterprise tools must be configured to exclude Company data from model training and third-party retention.

11. POST-EMPLOYMENT AND POST-ENGAGEMENT OBLIGATIONS

a. ***Survival.*** A Covered Person's obligations under this Policy survive the termination or expiration of their employment or engagement with the Powerus Group, for as long as the information at issue continues to qualify as Confidential Information. With respect to Trade Secrets, obligations continue indefinitely under the DTSA and NRS Chapter 600A.

b. ***Return or Destruction of Confidential Information.*** Upon the termination of employment or engagement for any reason, or upon request by the Company at any time, each Covered Person must promptly:

- i. Return to the Company all originals and copies of Confidential Information in any form or medium (physical or electronic) in their possession, custody, or control;
- ii. Permanently delete all Confidential Information from any personal devices, personal cloud storage, and personal email accounts; and
- iii. Certify in writing, upon request by the General Counsel, that all such information has been returned or destroyed. Classified Information and CUI must be returned or destroyed in

accordance with the Government Data Protection Policy and applicable government procedures rather than through the personal-deletion process described above.

c. *No Retention or Transfer.* No Covered Person may retain any copy of Confidential Information, or transfer Confidential Information to a personal storage medium or account, in anticipation of or in connection with their departure from the Powerus Group.

d. *Assistance After Departure.* Former Covered Persons must cooperate reasonably with the Company's requests for assistance in connection with any investigation or litigation relating to matters within their former areas of responsibility, subject to their legal rights.

e. *New Employer Obligations.* A Covered Person leaving the Powerus Group is responsible for ensuring that they do not use or disclose any Confidential Information in connection with their new employment or engagement. The Company reserves the right to notify a departing Covered Person's new employer of the existence and scope of the Covered Person's confidentiality obligations.

12. REPORTING SUSPECTED BREACHES

a. *Duty to Report.* Every Covered Person has an affirmative obligation to report any known or suspected unauthorized access to, disclosure of, or use of Confidential Information — whether by themselves, another Covered Person, or any third party — to the General Counsel promptly after becoming aware of it. Early reporting is critical to limiting damage and satisfying any mandatory breach notification obligations.

b. *How to Report.* Reports should be directed to:

Nicole Nan, General Counsel — legal@power.us

Jim Biehl, Chief Legal Officer — jim@power.us

For suspected breaches involving Classified Information or CUI, the Facility Security Officer must also be notified immediately and applicable government incident reporting requirements (including DFARS 252.204-7012 cyber incident reporting) must be followed.

Reports may also be submitted through the Company's Whistleblower Program.

c. *No Retaliation.* The Company will not retaliate against any Covered Person who reports, in good faith, a suspected breach of this Policy or any other potential violation of law. Retaliation against a good-faith reporter is itself a violation of this Policy and may violate applicable law.

d. *Self-Reporting.* A Covered Person who has inadvertently disclosed Confidential Information without authorization should self-report to the General Counsel immediately. Prompt self-reporting will be considered a mitigating factor in the Company's response.

13. DEFEND TRADE SECRETS ACT — IMMUNITY NOTICE

Pursuant to the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1833(b), the following immunity notice applies to all Covered Persons:

IMMUNITY NOTICE: *An individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (A) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual files any document containing the trade secret under seal and does not disclose the trade secret, except pursuant to court order.*

14. **REMEDIES FOR VIOLATIONS**

a. ***Company Disciplinary Action.*** Any Covered Person who violates this Policy is subject to disciplinary action, up to and including immediate termination for cause, regardless of whether any civil or criminal action is brought. Violations will be assessed in light of all relevant facts, including the nature and severity of the breach and whether the Covered Person self-reported.

b. ***Legal Remedies.*** The Company will pursue all available legal remedies for violations of this Policy, including:

- i. Injunctive relief under the DTSA (18 U.S.C. § 1836(b)(3)) and NRS Chapter 600A to prevent further disclosure or use of Trade Secrets or other Confidential Information;
- ii. Monetary damages, including exemplary damages of up to two (2) times actual damages for willful and malicious misappropriation under the DTSA and NRS 600A.050;
- iii. Recovery of attorneys' fees in cases of willful and malicious misappropriation or bad-faith claims;
- iv. Disgorgement of any profits derived from unauthorized use or disclosure; and
- v. Criminal prosecution referral for violations of 18 U.S.C. § 1832 (theft of trade secrets) or 18 U.S.C. § 1030 (Computer Fraud and Abuse Act).

c. ***Indemnification Limitations.*** Covered Persons who engage in unauthorized disclosure of Confidential Information in violation of this Policy will not be entitled to indemnification by the Company for any resulting legal liability, costs, or penalties.

15. **RELATIONSHIP TO OTHER POLICIES**

This Policy supplements and must be read together with the following Company policies, each of which contains additional obligations applicable to specific categories of information or specific circumstances:

- i. Insider Trading and Communications Policy — governs the handling and disclosure of MNPI and communications with investors and the public;

- ii. Blackout Period Policy — governs trading restrictions during periods of MNPI sensitivity;
- iii. Contract Review and Approval Policy — governs the execution of NDAs and other agreements involving third-party Confidential Information;
- iv. Export Control and ITAR Compliance Policy;
- v. Information Security Policy;
- vi. Document Retention Policy;
- vii. Code of Business Conduct and Ethics;
- viii. Whistleblower and Financial Integrity Policy;
- ix. The Powerus Employee Communications Handbook; and
- x. Government Data Protection Policy, which governs the identification, marking, safeguarding, transmission, and disposition of CUI, Classified Information, Federal Contract Information, and other Government Information.

In the event of any conflict between this Policy and a more specific policy governing a particular category of information, the more specific policy governs. In all cases, the more restrictive requirement applies.

16. ADMINISTRATION AND REVIEW

The General Counsel is responsible for administering this Policy, including distributing it to new Covered Persons, responding to questions, and maintaining records of acknowledged receipt. The General Counsel will present this Policy to the Audit Committee of the Board of Directors for review at least annually and will recommend amendments as necessary to reflect changes in applicable law, regulation, or Company operations.

The Company expressly reserves the right to amend or rescind this Policy at any time. Questions about this Policy should be directed to the General Counsel.

All Covered Persons are responsible for consulting and complying with the most current version of this Policy. The current version is maintained on the Company's intranet and is available from the Legal Department.

* * *

Acknowledgment Form Follows



POWERUS CORPORATION
CONFIDENTIAL INFORMATION POLICY
ACKNOWLEDGMENT FORM

I, the undersigned, acknowledge and certify that:

- (1) I have received and read the Powerus Corporation Confidential Information Policy (the “Policy”).
- (2) I understand my obligations under the Policy, including my duty to protect Confidential Information, to use it only for authorized business purposes, and to report any suspected unauthorized disclosure.
- (3) I understand that the Policy includes information about the DTSA immunity notice set forth in Section 13, and that I may be immune from criminal and civil liability for the limited disclosures described in that section.
- (4) I agree to comply with the Policy during and after my engagement with the Powerus Group.
- (5) I understand that violations of the Policy may result in disciplinary action, up to and including immediate 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

Print Name Legibly

Title / Department

Date

Please return signed form to:

Nicole Nan, General Counsel — legal@power.us

Jim Biehl, Chief Legal Officer — jim@power.us