# THE CADMUS GROUP
# INFORMATION TECHNOLOGY RULES OF BEHAVIOR (ROB)

The Cadmus Group (Cadmus) provides access to Information Technology (IT) resources (hardware, software, and data) to its employees and contractor staff for the completion of assigned duties and responsibilities. ***Cadmus's Information Technology Rules of Behavior*** are derived from twenty (20) Cadmus compliant IT Security Policies. These rules of behavior do not set policy but instead summarize and amplify existing IT Security Policies. Individuals who are authorized to use Cadmus IT resources must comply with Cadmus policies in the *Employee Handbook* and Rules of Behavior.

## End User Responsibilities

- **Use Cadmus laptops**: I will use Cadmus laptops and computers only for lawful and authorized purposes.
- **Compliance**: As a user of Cadmus issued equipment and/or systems, I will comply with safeguards, policies, and procedures to prevent unauthorized access to Cadmus information systems.
- **Expectation of Privacy**: I recognize that I am accountable for my assigned User ID and password. I also understand that each user must have a unique ID to access Cadmus systems and that I have no expectation of privacy while using Cadmus equipment, internet connection, e-mail services, or data storage. I will **not** store personal data on Cadmus equipment.
- **Security Incident Handling and Reporting**: I will report suspected or actual IT security incidents and privacy breaches, which include stolen, lost, destroyed, or compromised Cadmus IT equipment, mobile devices, Portable Storage Device (PSD) and/or Bring Your Own Device (BYOD) mobile devices. I will report all incidents immediately, or as soon as I become aware of them, to alert Cadmus IT of a potential security incident. I will report incidents by opening an IT ticket, navigating here.
- **Laptop best practices**: I will log-off or lock my computer whenever I leave the workstation unattended, and I will use a password-protected screen saver.
- **Use of E-Mail**: Threatening, obscene, or harassing messages are not allowed. I will not open unsolicited or suspicious e-mail messages or their attachments, forward chain mail, or generate or send offensive or inappropriate e-mail messages, graphical images, or sound files. I will limit distribution of e-mail to only those who need to receive it.
- **Anti-Virus Protection**: I will keep my anti-virus software up to date while accessing IT systems and resources using Cadmus-issued/non-Cadmus equipment. When my workstation begins an update of its anti-virus software, I will let the update finish. I will know the source before using external media or downloading files and will scan files for viruses before opening them.
- **Teleworking (Working from home)**: I will protect my personal devices with antivirus and will keep the programs and operating systems up to date if I use those systems to access Cadmus resources. I will configure my home Wi-Fi with encryption and a strong password and will change personal router login and password periodically (quarterly/semi-annually). I will use corporate services for E-Mail, Messaging, and all other work and use a personal device for personal internet and personal computer processing needs. When using personal devices to connect to the Cadmus network, I will comply with requirements stated in the *Cadmus BYOD Policy*.
- **Data Backups**: I will ensure that data is backed up, tested, and stored safely. If the data is stored on a network drive, this is done automatically. If it is stored on the local hard drive, I am responsible for backups. ***Note: Data stored under Cadmus user's OneDrive folder in Cadmus-issued devices is automatically backed up.***
- **Protection of copyright licenses (software)**: When using Cadmus-issued equipment, I will not download or install any software application(s) on systems without prior IT approval. I understand that all software must be properly licensed prior to installation on any Cadmus-owned equipment and that unauthorized copying of copyrighted software is prohibited.

- **Use of Equipment (Limited Personal Use)**: I will complete on-boarding orientation and all mandatory IT training regarding the use of Cadmus-issued equipment and IT resources. I understand that I can use Cadmus-owned equipment during non-working hours (before scheduled work hours, lunch times, and after work hours) for personal use with at least the following restrictions.
    - Personal use of Cadmus-issued equipment and IT resources must not incur any additional costs to Cadmus and/or violate any local, state, federal laws, or Cadmus policies.
    - Activities **not permitted** on Cadmus-owned IT resources include, but are not limited to the following:
        - private commercial business activities or profit-making ventures
        - viewing, obtaining, creation, distribution, or storing of sexually explicit material
        - violation of any statute or regulation, including applicable copyright laws.
    - I will **not** install personally purchased software on Cadmus-issued equipment.
    - I will **not** use Peer to Peer (P2P) connection sharing for transferring copyrighted files.
- **Remote Access**: I understand that some remote access, especially to specific systems, requires additional approval from my manager. I will review and comply with all aspects of Cadmus's policies regarding remote access. These rules of behavior apply for all remote access.
- **Data Destruction**: I will properly dispose of unneeded data. I will not throw sensitive hard copies into a wastebasket.
- **Cadmus Cyber Security Awareness Training**: I understand I am required to complete the Cyber Security Awareness and Information Security Training course annually.
- **Generative Artificial Intelligence (AI) Guidance**: I understand I am required to adhere to the following preliminary guidance established for the use of generative AI software.
    - I will **not** use AI tools for Client/Project Delivery. Use only as directed by client or Project Manager.
    - I will **not** use AI tools to prepare proposal responses.
    - I will **not** enter any sensitive data (Client information or PII) into AI tools.
    - I will **not** rely blindly on the results of an AI query or use direct results for client deliverables.
    - I will **not** use Cadmus credentials (Email & Password) to register to AI tools/software services.
- **Tik Tok Guidance**: If I use my personal device to work on U.S. Government contracts, I will remove/uninstall the TikTok (owned by ByteDance) application from my device.

## Management Responsibilities

Cadmus Senior Management, Human Resources, Supervisors, CIO staff, and Application/System Owners are responsible for ensuring that adequate protection is provided to IT resources which come with an appropriate mix of managerial, operational, and technical controls. Specifically, Management is responsible to ensure:

- **All employees/contractors** performing work on behalf of Cadmus:
    - Have undergone an appropriate background check or security clearances, (as appropriate), and
    - Are trained in the protection and security of information, data, software, hardware, and systems
- **Employee/contractor access privileges** are granted to information and systems commensurate with the employee/contractors' duties and responsibilities, specifically:
    - Access will be granted to information systems based on role.
    - Access privileges shall be removed when the need expires or within 24 hours of separation from Cadmus
- **All employees/contractors** have current knowledge of these Rules of Behavior, including specialized rules for specific data sets and systems that govern the use of workstations, the network, databases, and other systems.
- **All** Cadmus employees/contractors are informed regarding the existence of and application of these rules.

By signing below, you are requesting authorization to use Cadmus systems and IT resources and agreeing to comply with Cadmus Policies and the specific Rules of Behavior listed above.

**Printed Name (optional if digitally signed)**

**Date (optional if digitally signed)**

**Signature**