Kratos Defense & Security Solutions
Physical Security and Cybersecurity Supplement

The purpose of this supplement is to provide additional guidance regarding Company policies and required procedures related to physical security and cybersecurity not otherwise covered within the Kratos Employee Handbook of a local office. Nothing in this supplement is intended to conflict with applicable law. If anything in this supplement conflicts with the laws that are applicable to a local office, the applicable law takes precedence and any conflicting portion of this supplement will have no force or effect.

COMPANY PROPRIETARY

Protection of Company Property.

- Protection of Tangible Assets and Property. We must all use the Company assets entrusted to us carefully and protect these assets from loss, theft, or misuse.
  - Do not sell, lend, transfer, give, or dispose of Kratos' assets without proper authorization.
  - Use assets appropriately and carefully in your work and protect them, for example, by closing drawers and cabinets.
  - Notify your Company facilities, security, procurement, or risk management representative (or the equivalent) immediately if Company property is lost or stolen.
  - Use government*-furnished property only to serve legitimate government purposes under a government contract or subcontract.
  - Do not allow unauthorized visitors onto Company facilities without an escort and a visitor badge. Ensure that all visitors sign the visitor log at your facility.

* The word "government" is used generally in this supplement and does not apply to any specific government.

- Protection of Proprietary Information and Business Relationships. We work in highly competitive industries. Confidential and/or proprietary information to which you have access during your work, whether in your memory, in writing, or in electronic form, is Company property.

HERE'S AN EXAMPLE

Confidential and/or proprietary information about our business includes information about our profit margins, prices, contract terms, CMMC certification, and technology, and certain information about our customers.

We've spent money and effort to develop this valuable information and to keep it from general distribution, and unauthorized disclosure of it could cause serious business and financial losses to us. When you leave your employment with Kratos, you must return this information to us,

and you may not use or disclose Kratos' confidential and/or proprietary information for the benefit of anyone else.

- Protection of Intellectual Property Developed by the Company. The Company has developed certain proprietary technologies, processes, designs, systems, solutions, and services for sale or use in performing services to clients. These proprietary tools are the Company's valuable "intellectual property." To preserve this value, do not share, sell, or license such proprietary tools to others without the Law Department's involvement.

- Use and Protection of Licensed Software and Data Products Licensed by the Company; Copyrights. Most of the software used by the Company is covered by some form of license agreement that describes the terms, conditions, and uses allowed for that software.

It is our policy to respect copyright laws and observe the terms and conditions of any license agreement. Be aware of the restrictions on the use of software and abide by those restrictions. Do not copy or share software on Kratos computers without first checking with the IT Department.

EMPLOYEE CONDUCT

Employee Conduct Expectations

Performance that falls below expected standards and unacceptable conduct may impact an employee's compensation as permitted by law, work assignment, and ability to transfer within the Company, and may lead to discipline. While it is impossible to identify every type of improper conduct that may lead to discipline, examples include violating the Security and Acceptable Use of Information Technology Equipment and Systems Policy.

It is critical for the Company to preserve and protect its trade secrets and Confidential Information, as well as the confidential information of any government, customers, suppliers, and third parties. All employees are responsible for ensuring that proper security is maintained at all times.

Controlled Unclassified Information

Controlled Unclassified Information ("CUI") is information pertaining to a U.S. Department of Defense contract that requires safeguarding or dissemination controls pursuant to and consistent with applicable U.S. law, regulations and government wide policies but is not classified. A non-U.S. entity may be approved to receive CUI when deemed appropriate by a U.S. government agency. It is the responsibility of all Kratos employees that create, receive, store, or manage CUI to secure CUI in accordance with Kratos Global Policy OA 30 ("Securing Controlled Unclassified Information"), Global Policies as may be adopted by the Corporate Information Technology Department, and procedures adopted by their business unit.

Confidential Information

Confidential Information is any information of a confidential or secret nature that may be disclosed to employees or created, discovered, received, or learned by employees that relates to the business of the Company or to the business of any parent, subsidiary, affiliate, customer, supplier, or vendor of the Company, or any other party with whom the Company agrees to hold information in confidence ("Confidential Information"). By way of illustration but not limitation, Confidential Information includes: (i) trade secrets, inventions, mask works, ideas, processes, formulas, algorithms, software, source and object codes, data, programs, other works of authorship, know-how, improvements, discoveries, information relating to products, processes, designs, drawings, test data, methods, samples, improvements, developments, designs and techniques, data, compilations, blueprints, plans, audio and/or video recordings and/or devices, information on computer disks, software, tapes, printouts and other printed, typewritten or handwritten documents, specifications, strategies, systems, schemas, methods; (ii) information regarding plans for research, development, new products, marketing and selling, business plans, budgets and unpublished financial statements, licenses, prices and costs, suppliers and customers; (iii) information regarding the skills of other employees of or consultants to the Company; and (iv) such other information that (a) derives independent economic value, actual or potential, for not being generally known to the public or to other persons, or (b) is the subject of efforts to maintain its secrecy, all of which is, previously, presently, or subsequently disclosed to employees during their period of employment with the Company. Confidential Information of customers and clients in the Company's possession is considered Confidential Information for the purposes of this policy. The foregoing are only examples of Confidential Information. If employees are uncertain as to whether any particular information or material constitutes Confidential Information, they shall seek written clarification from their Manager or HR Representative.

Security Procedures

To avoid loss of Company property, each location maintains and promulgates security procedures, which include maintaining control of entrances, exits, restricted areas, document control, and record keeping. Specific procedures regarding the protection of Company property, traffic throughout the facilities, and designation of restricted areas apply at each location and are generally posted on Company bulletin boards. Employees are expected to abide by all Company security procedures.

Avoiding loss or theft of trade secrets and of Confidential Information is an important part of each employee's job. Accordingly, employees must observe good security practices and are expected to keep all such property secure from outside visitors and all other persons who do not have legitimate reason to see or use it. Employees may not remove Company property, including trade secrets and Confidential Information, without authorization. Failure to adhere to such policies may be grounds for disciplinary action, which could include dismissal.

Given the sensitivity of trade secrets and Confidential Information, employees may only dispose of them by secure methods approved by the Company. If an employee has any doubt or

question about how to handle trade secrets or Confidential Information, the employee should consult with the Company's IT Department.

Handling the Press and Other Outside Entities

If any outside entity, such as a news agency or media, investor, or business analyst or anyone else asks an employee to comment or provide information on behalf of Kratos, including regarding its financial statements or business dealings, only the CEO, CFO, and their designees are authorized to make public communications on behalf of the Company, in order for the Company to consistently deliver an appropriate message and to avoid giving misinformation in response. All other employees should refer such inquiries to their manager, who will ensure that they are relayed to authorized representatives. Nothing in this policy shall be interpreted to interfere with employees' rights under any law that permits employees to freely discuss aspects of their employment.

USE OF TECHNOLOGY

Security and Acceptable Use of Information Technology Equipment and Systems

Our Company is a government contractor and a leading technology, intellectual property, and proprietary product and solution company focused on the United States and its allies' national security. Our areas of expertise include unmanned aerial drone target systems, unmanned combat aerial systems, satellite communications, microwave electronics, cyber security/warfare, missile defense, and combat systems. This means that virtually any given day-to-day business email or communication can contain extremely sensitive information. We abide by all contractual obligations to maintain confidentiality and security of the information entrusted to us, and that is essential to our business services. In addition, this policy sets forth expectations related to employee use of the Company's computer and IT systems and resources (collectively, "Business Systems"). In sum, employees are expected to use our Business Systems in a responsible manner that reflects their understanding and appreciation of their obligation to safeguard the extremely sensitive information, including CUI, in the Company's possession. Failure to do so will result in disciplinary action, which may be termination.

Protecting the Company's Business Systems and Information

Employees may be assigned Company equipment for use on the job. Employees will care for and keep all such equipment in good condition. All Company owned equipment must be returned upon termination of employment.

Access to Kratos Business Systems on the IT Services Network is password restricted to protect these systems against unauthorized access. Specific exceptions to networks other than the IT Services Network will be explicitly granted on a case-by-case basis. It is each employee's responsibility to ensure their password(s) remain confidential. Employees must not share their passwords with others. If an employee believes his or her password(s) has been compromised, he or she should change it immediately and notify IT.

All Kratos computers attached to the IT Services Network will be loaded with the company approved IT Security Suite. No computer, regardless of function, will be allowed on the IT Services Network without the IT Security Suite. Included in the IT Security Suite are tools to protect the integrity, availability, and confidentiality of data and intellectual property stored on and processed by the computer.

Kratos' computers are loaded with approved standard software configurations designated by job need, project requirement, and security safeguards. Software provided with these computers is licensed by Kratos from various software vendors. These software licenses generally prohibit the copying and use of the software by unauthorized users, and it is the responsibility of Kratos employees to comply with the license agreement, including by not copying and/or distributing copyrighted software. Adding to or removing software from Kratos computers should only be accomplished with the assistance of the IT Department. Employees must not install any personal software on any Kratos Business Systems. The IT Department conducts regular audits to ensure that unauthorized or illegally copied software is not used by Kratos employees. During such audits, any unlicensed and unapproved software will be removed. Employees knowingly using unlicensed or unapproved software may be subject to disciplinary action.

Other networks may be provided at the sole discretion of Kratos IT Services for various purposes as required (Guest network, lab networks, equipment/utility networks, etc.), which are limited in use and services provided. Any system accessing an alternate network must be explicitly and appropriately approved by local business management. No system will be permitted to bridge to multiple (connect to more than one at a time) Kratos networks.

When travelling with Kratos IT Equipment, the following applies:

- Kratos devices, such as Company-owned laptops, tablets, or portable data processing or storage devices, shall not be taken on international (i.e., out of your resident country) travel unless encrypted using approved encryption software.

- For both domestic (within your resident country) and international travel, the Company's approved secure Mobile Device Management ("MDM") must be loaded on any Company-owned IT equipment (such as tablet or smartphone) that is taken on such travel.

- The Company may grant exceptions for un-encrypted laptops, although they carry significant increased risk both to the employee and Kratos. Business divisions must have sufficient controls in place to manage their exception process. In addition, note that:

    - Business units are responsible for providing blank un-encrypted laptops to their employees who need to travel internationally for business reasons.
    - Un-encrypted laptops will not have Kratos domain access, VPN clients, the Outlook client, or other IT Services applications running on them.
    - All network services should be accessed through webmail or one of our secure portals.
    - All accounts on the un-encrypted laptop should be local accounts and follow Kratos

password complexity policy.

- These un-encrypted laptops must not be placed on the IT Services Network upon return until cleared by Kratos IT.

- Use personal charging adapters and cables by directly plugging them into electrical outlets. Do not use public USB ports to charge your devices.

- Employees are responsible for ensuring that Kratos devices remain in their possession, or are secured, at all times. Employees are responsible for immediately reporting to Kratos IT anything suspicious related to the device or if such device is lost or stolen. If a device is suspected of being stolen, the employee should also contact local authorities and file the appropriate report(s).

When remotely accessing Kratos resources, the following applies:

- Kratos IT will provide Virtual Private Network ("VPN") client software for those employees that need to work from facilities not otherwise connected to the Kratos IT Services Network and using Kratos devices. Employees that are not using Kratos issued devices must have the business unit manager and the CIO approve the employee's use of the VPN client software on such device. The same policies that govern computers connected directly to the Kratos IT Network apply to remote computing.

- Please note that at no time should the VPN client be used on a personal or non-Kratos owned device.

- Any use of non-approved VPN solutions in order to gain access to the Kratos network is prohibited and will be subject to disciplinary action.

Safeguarding extremely sensitive information, including by preventing cyber-attacks, and avoiding loss of Intellectual Property, is the responsibility of all users of Kratos IT Equipment. Kratos is frequently targeted by hackers and other cybercriminals. All employees must be vigilant in protecting the Company and its Business Systems against cyber-attacks. To this end, all Kratos employees must always observe the following:

- Never click on or open links or attachments that you are not 100% confident are legitimate.

- If you do not recognize the sender or if an email looks suspicious, do not open links and attachments and report it to IT Security (badmail@kratosdefense.com).

- Never disable the IT Security Suite on a Kratos computer.

- Circumventing security protections is strictly prohibited. This includes working around or disabling passwords or virus detection; using anonymizing services; or using a web proxy to visit sites that would otherwise be filtered.

- Any remote Kratos computers should limit direct internet access by maintaining a VPN

client connection to the Kratos network whenever possible in order to limit security exposure.

- Safeguard your computer and all mobile devices used for work purposes when you are traveling and in public spaces.

All devices connected to the Kratos IT Services Network must be approved by the CIO. Under no circumstances should a personally owned device (for example computers, wireless access point, mobile phone, tablet, etc.) be joined to the Kratos IT Services Network.

Company Ownership and Access

Email messages and other electronically stored documents and data pertaining to or embodying Company business, wherever stored, are Company property. Such messages, documents, and data should be preserved in accordance with Company retention policies and made available to the Company upon request.

To safeguard the extremely sensitive information with which we regularly conduct business, Kratos retains the right, in its sole discretion, and without further notice, to access, monitor, review, remove, disclose, and/or control any aspect of access to or use of its Business Systems, including any and all data, email, files, instant messages, internet usage, or documentation recorded in or using those systems. All communication to and from any Kratos Business System is monitored and may be logged and/or recorded by the Company. Kratos' rights under this paragraph are subject to applicable privacy laws, which may prohibit or limit the activities described herein.

Appropriate Use of Company Business Systems

To safeguard the extremely sensitive information with which we regularly conduct business, Kratos must restrict usage of its Business Systems when not related to the Company's business. As such, Business Systems may not be used to: solicit commercial ventures, religious or political causes, outside charitable organizations (unless sponsored by Kratos), or other non-job-related solicitations; engage in any conduct that is prohibited by law or that violates the Kratos Code of Legal and Ethical Conduct or the Equal Employment Opportunity, Anti-Harassment, and Anti-Retaliation Policy, or if those policies are not applicable, any local policy on these topics. In addition, Kratos Business Systems should not be used to send (upload) or receive (download) material, or to participate in activities, any of which involve harassment, gambling, web-based surveys, non-work-related subscription-based services, email attachments from unknown senders, forwarding of company mail to non-company accounts, or social networking.

Uploading any CUI, company information or data, including email or email forwarding, to unapproved public or private cloud storage or email services (Apple iCloud, Drop Box, Amazon Cloud Drive, Google Drive, etc.) is strictly prohibited. Data should only be transferred via systems or devices approved or provided by Kratos IT. Only Kratos standard USB storage devices are authorized for use in Kratos systems.

To safeguard the extremely sensitive information with which we regularly conduct business, sensitive copyrighted materials, trade secrets, Confidential Information, confidential financial and other business information, or similar materials should not be transmitted outside of the Company by any means without prior written authorization from an employee's manager, who will determine whether additional authorization is required.

Employees should make clear in any online discussions related to the Company, including blogging, posting, tweeting, or any form of communication on external social media services and systems, that they are not speaking for the Company (unless they are authorized by the CEO or CFO to speak on behalf of Kratos or its businesses and divisions). In addition, any such employee communication outside of Kratos Business Systems is prohibited if it discloses trade secrets or Confidential Information. Likewise, employees must make clear in their personal online activities that relate to the Company's business interests, that they are not speaking for the Company. To protect Company Confidential Information, employees should be careful with their connections with unknown users on social networking sites. Social media should not be used in a way that violates any other Kratos Policies or employee obligations, such as providing references or recommendations on sites (i.e. LinkedIn) in such a way that they can be attributed to Kratos. Posting of photos of co-workers without their express consent is prohibited.

Any exception to the Security and Acceptable Use of Information Technology Equipment and Systems policy must be approved by the CIO in writing.

Recording Devices in the Workplace

Our Company is a government and commercial contractor and a leading technology, intellectual property, and proprietary product and solution company focused on the United States and its allies' national security. Our areas of expertise include unmanned aerial drone target systems, unmanned combat aerial systems, satellite communications, microwave electronics, cyber security/warfare, missile defense, and combat systems. This means that on a day-to-day basis, any given business email, discussion, or communication in our work environment can reflect or contain extremely sensitive information.

The nature of this information, as well as our obligations under government contracts related to maintaining confidentiality and security of the information entrusted to us, and that is essential to our business services, requires all employees to protect and guard against the disclosure of Company Confidential Information (defined in the Confidential Information and Trade Secrets – Obligations of Kratos Employees Policy).

As part of this protection, unless expressly authorized by the Company as below, Company policy prohibits employees from taking audio recordings, video recordings, or photographs within the workplace or during or in connection with work-related communications, regardless of where the participants are located at the time, including of individuals, conversations, communications, files, data, equipment, or facilities. For example, employees may not use the built-in camera or video/audio recording capabilities of smart phones, tablets, computers, or

other devices to photograph or record any conversations or any meetings conducted in person or by use of remote technology during the performance of Company business without first obtaining express authorization from the Company as described below. This policy encompasses employee use of cameras, camcorders, tape recorders, smart glasses, smart watches, or the audio or video recording functions of cellular phones or any other recording devices in the workplace. Likewise, in the workplace or during or in connection with work- related communications, regardless of where the participants are located at the time, employees are specifically prohibited from wearing Google Glass, Samsung Galaxy Gear, or any other "wear- able" audio or video recording devices, even when the recording capabilities are not in use and regardless of whether the recording capabilities are activated, unless prior authorization has been obtained pursuant to this policy.

Requests for authorization should be submitted to an employee's manager. Authorization may be granted to an employee when the manager determines that a specific business purpose may be served and use of the device will not disclose or threaten disclosure of Confidential Information, including extremely sensitive information. In addition, because many of the countries in which the Company has business operations have laws prohibiting recordings or similar surveillance absent the consent of all parties to a conversation or communication, before the Company's authorization may be applied to allow a recording or photography, all participants and/or parties to the meeting, conversation, or communication that is to be recorded and/or photographed must (i) be informed of such recording and/or photography before the meeting, conversation, or communication begins, and (ii) consent to the recording, either in a writing provided in advance to the authorizing manager or, if a recording, on the recording.* Once granted, authorization is limited to the particular recording/photography event for which authorization was provided.

The use, possession, or wearing of audio or video recording devices in the workplace for non-business purposes is generally prohibited. Requests for an exception to this prohibition must be submitted to Human Resources for review with the Law Department. Please note: This policy does not prohibit employees from possessing, while at work or conducting business, a smartphone or similar device, so long as it is used for personal reasons only, and it is not used for audio or video recording, or photographing, in violation of this policy. However, this limited exception allowing possession of smartphones or similar devices, or the authorization to use, possess or wear an audio or video recording device in the workplace, may be revoked at any time if, in either case, such device(s) is/are used in a manner that violates this policy.

* Kratos does not consent to photographs or video or audio recordings of any business-related meetings or discussions without a manager's prior authorization as discussed above.

HEALTH, SAFETY, AND SECURITY

Physical Security

Kratos is concerned for the security and well-being of all its employees. A secure working environment with controlled access to sensitive or dangerous areas is provided at most company

facilities. At various locations, automated fire alarm and sprinkler systems are in place and tested at scheduled intervals. At various locations security cameras have been installed throughout the building to monitor activity during and after business hours.

Security awareness is an individual responsibility. The proper use of security equipment and systems, and a cautious approach to unusual or suspicious situations, will help all employees remain safe and secure. Any unusual or suspicious situations should be reported immediately to the employee's supervisor or the next available supervisor in the event his or her own supervisor is unavailable. To assure the safety and security of Company employees, its visitors, and its property and to ensure that only authorized personnel have access to the Company facilities, the following policies have been adopted:

- Employees are required to wear their badges so that they are visible when in Kratos facilities.

- Non-employees must sign in and out according to the prescribed register. All non-employees on Company property must be issued a badge by the appropriate administrative associate or receptionist, except as discussed below, uniquely designated as "Visitor," and the visitor badge must be returned to the issuing party the same day of the visit when signing out.

- Suppliers and Delivery Personnel: Truck drivers will use their Bill of Lading as an acceptable ID; however, such persons shall not be permitted outside their normal areas of pick-up and delivery without being escorted by an appropriate associate. Delivery personnel (i.e., UPS, Federal Express, etc.) and facility maintenance personnel will be permitted to make their deliveries to or work in the appropriate areas without a badge, provided they do not go outside normal areas of service.

Contractors and Temporary Employees: Contractors working temporarily for Kratos will follow screening practices as determined by Human Resources and in a manner consistent with applicable law, and as appropriate will be issued badges with the individual's picture or a visitor badge.

All non-employees visiting Company property will be required to comply with all safety rules, regulations, and policies of the Company while on Company property or in Company vehicles. Unless designated as not requiring an escort, all visitors who are not Kratos personnel must be escorted by a Kratos personnel host. It is the responsibility of the Kratos personnel host to ensure that the visitor is monitored at all times to ensure they are not physically accessing any organizational resources that they have not been authorized to access. Organizational resources include, but are not limited to information systems, equipment, and the respective operating environments.