1 PURPOSE

To establish Standard Operating Procedures for how to handle Unauthorized Disclosure (UD) of Controlled Unclassified Information (CUI) in the event a KNC employee, independent contractor, or subcontractor has been determined to have disclosed CUI, whether intentionally or unintentionally, to a non-authorized recipient.

2 GENERAL POLICY

KNC Strategic Services Acceptable Use Policy and Processes for Safeguarding CUI SOP

3 PROCEDURE FOR HANDLING AN UNAUTHORIZED DISCLOSURE (UD) OF CUI

In the KNC Processes for Safeguarding Controlled Unclassified Information SOP, UD is defined as:

- Unauthorized disclosure of CUI occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls. This may include intentional or unintentional errors in safeguarding or disseminating CUI. This may also include the incorrect marking of CUI.
- DoD defines UD as "Communication or physical transfer of classified or controlled unclassified information (CUI) to an unauthorized recipient."

The KNC Privileged User Agreement contains the following agreement:

- It is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information.

Definitions:

- **Compromise:** A security incident in which there is a UD of controlled unclassified information
- **Data Spill:** The willful, negligent, or inadvertent disclosure of CUI across computer systems accredited at a lower classification level than the data being entered.
- **Espionage**: Activities designed to obtain or transmit CUI in order to harm the United States or to provide advantage to a foreign nation or transnational entity.
- **Leaks**: When CUI is deliberately disclosed (media).
- **Unauthorized Recipient:** Information wherein individual disclosed classified information and/or controlled unclassified information to unauthorized person or persons resulting in administrative action, referral for criminal and/or CI investigation, and/or resulted in the suspension or revocation of eligibility.

Training

CDSE UD Training: https://securityawareness.usalearning.gov/disclosure/story.html

In the event of a suspected UD, KNC will conduct fact-finding and analysis, and gather the necessary evidence. This process must be completed within 10 business days of the discovery of the UD.

Procedure In the Event Of A Suspected UD

1. Identification –
    a. Notification by the observer of suspected UD of CUI to KNC executives
2. Triage – within 72 hours
    a. Secure any materials related to the UD

b. Notify the appropriate authorities, vendors, prime contractors, and clients where required

3. Preliminary Inquiry – within 10 business days
   a. Conduct fact finding and analysis to determine the facts related to the incident
   b. Document who, what, when, where, and how
4. Damage Assessment – within six months of UD
   a. Conduct a detailed analysis to determine the impact of the compromise
   b. Document the effects on our business, systems, people, partners, and clients

Reporting

DOD Unauthorized Disclosure Project Management Office Contact Information:

- **Phone: 571-357-6875**
- **Email:** dcsa.quantico.hq.mbx.ditmac-unauthorized-disclosure@mail.mil

DIBNET

To report a mandatory cyber incident to the DoD, logon to DIBNET at https://dibnet.dod.mil/portal/intranet/ and file a report within 72 hours of discovery.

- Mandatory incident reporting under DFARS 252.204-7012
- Malicious software, affected system images, packet capture, and other data relevant to the reported cyber incident must be preserved for 90 days to allow time for DoD to request the data in order to conduct a damage assessment or decline interest.

4 RELATED DOCUMENTS / AUTHORITIES

1) DoD CMMC Program
2) Information Security Oversight Office
   - Controlled Unclassified Information Unauthorized Disclosure
3) NIST Special Publication 800-171

5 REVISION HISTORY

Resource(s)	Date	Version	Description
KNC Strategic Services	2/20/2026	Original	Original