Personally Identifiable Information (PII) Reporting Actions

The term PII means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, employment history or information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

1.Contact your **privacy coordinator (475-7122/7888)** or supervisor as soon as you suspect or have an actual loss or compromise of PII.

2. Make an initial report of all incidents involving actual or suspected breaches/ compromises of PII to **https://us-cert.gov** within one hour of discovery.

3. Report all incidents involving actual or suspected breaches/compromises of PII to the **HQ Army Privacy Office** within 24 hours of discovery at usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil by using DD Form 2959 or via PATS (Privacy Act Tracking System).

4. Contact the USAREUR Privacy Officer as well as continue to follow existing internal command procedures to notify local command officials.

For more information please see: https://www.rmda.army.mil/privacy/PII/PII.html

Phishing / SMS phishing Smishing Emails or Text Messages

Do Not: Reply to the message / Follow its instructions / Forward to another / Click on any embedded links.

Do: Contact your local IT Support Staff
Call 119/ESD to create a ticket
Preserve the Phishing email by:

1)Open Phishing Email
2)Go to File - Save As - Outlook Message Format - Unicode (*.msg) and Save.
3) Create a new email.
a. Attach a copy of the saved phishing email
b. Add the <Subject Line> "Phishing Email Submission"
c. Make out the recipient as usarmy.wiesbaden.5rcc-eur.list.phishing-reporting@mail.mil
d. Send the email.
4). Permanently delete the phishing email by highlighting it and pressing Shift+Delete.
Local S-6 office should send out a warning email to those users within their area.

USAG Bavaria Computer Incident Response Contact Information:

Cybersecurity Manager: 526-6002

Grafenwoehr-Vilseck S6: 526-6001/6004

Hohenfels S6: 520-5862

Garmisch S6: 440-3222

Enterprise Service Desk (ESD): 119

Computer Incident Handling and Reporting Procedures

12 April 2018

U.S.ARMY EUROPE

U.S. ARMY GARRISON BAVARIA

Incident and Intrusion Reporting Overview

Incidents and intrusions may be the result of deliberate malicious activity or the result of accidental mishandling of government equipment and information. In either case, significant damage to the Army's security posture can be the result. It is imperative that timely, mindful, and informed action be taken to ensure the safeguarding of Army information. This quick reference guide will give you the information needed to report incidents or suspected incidents in the proper manner.

EXAMPLES OF REPORTABLE INCIDENTS:

1. Anti-Virus alerts indicating a worm, virus, Trojan, or other infection.
2. Personnel alerting you about virus emails coming from your account.
3. Suspicious email in which you *responded to, clicked a link, or opened an attachment from.*
4. Occurrence of multiple pop-ups from your browser with inappropriate or other unsolicited content.
5. Unexpected events in your daily work routine (system slows to a crawl for no apparent reason, repeated system crashes and error messages, inability to open files or run applications).
6. Unexplained modifications to your background, files, or applications.
7. Presence of suspicious files, shortcuts, or programs on your system.
8. Witness the use of unauthorized systems or devices on the network.
9. Observe a Spillage/(UDCI) (Unauthorized Disclosure of Classified Information) on the UNCLASS network.
10. Note: The above list is not all inclusive. If you suspect malicious or suspicious activity **ALWAYS REPORT IT!**

Incident and Intrusion Reporting Actions

If you suspect you are involved in a computer incident or intrusion you must perform the following actions:

1. Cease Operations **IMMEDIATELY!**
2. Contact your Local IT Support Staff **& Call 119 to submit a ticket**.
3. DO NOT turn off your computer or disconnect the network cable.
4. Restrict physical access to the Information System or media until your IT Support Staff arrive.
5. **NEVER** perform investigative actions on your own.
6. Turn off the monitor and place a "Hands Off" notice over the computer monitor to notify people not to tamper with the system.
7. If an Unauthorized Disclosure of Classified Information (UDCI) / spillage is involved, follow the instructions at: (USAREUR iAssure: https://intranet.eur.army.mil/hq/iassure/CND/IR/SitePages/Incident%20Response.aspx) and work with your Security and IT Support Staff personnel.

Army Law Enforcement (LE) and Counterintelligence (CI) have highlighted the importance of protecting computer systems under investigation from modification and/or premature rebuilding. This protection ensures the integrity of crucial data required to defend U.S. Army networks, and to preserve evidence and proper chain of custody during LE/CI investigations. Incident responders must strictly follow forensic protection measures and chain of custody procedures.

Unauthorized Disclosure of Classified Information (UDCI) Reporting Actions

The majority of UDCI incidents result from careless methods, shortcuts, or untrained users who have intentionally or accidentally compromised sensitive and classified information vital to national security and operational processes. Follow these quick reference guidelines in the event of a UDCI:

DO:

- Isolate and guard the affected Information System (IS) immediately.
- Disconnect network connections.
- Implement your Command's spillage incident response plan immediately **(contact your Security Manager**
- **526-3020/3018/3015).**
- Restrict physical access to the computer or media until your Security Manager provides guidance.
- Complete initial unit information and Immediate Action Checklist (provided by Security Manager).
- Provide Immediate Action Checklist to your security Manager.

DO NOT:

- Investigate actions on the IS until authorized by Commander or information security personnel.
- Contact any commercial Internet service provider (ISP) or ISP account identified.
- Confirm or deny a spillage incident occurrence to the public.
- Confirm or deny the compromise of sensitive or classified information to the public.
- Delay implementation of containment procedures awaiting notifications of key personnel.