(when filled in) CLASSIFICATION //_____//

# Tyndall Network Users Quick Reference Card

*THINK OPSEC! DO NOT DISCUSS CRITICAL OR CLASSIFIED INFORMATION VIA UNSECURE MEANS*

## Your Unit Cybersecurity Liaison (CL)

Primary:_____ DSN:_____

Alternate: _____ DSN:_____

## Wing Cybersecurity Office

DSN: 523-2545 E-Mail: 325FW.cybersecurity@us.af.mil

## Account Locked Out?

Contact your Unit CL for assistance

**IAW DAFMAN 17-1307, the introduction of personally owned hardware, software, or both to an information system without cognizant AO approval is a violation of the information system user agreement and subject the user to repercussions outlined in the information system authorization package and may result in the loss of user access.**

## Cyber Awareness Challenge Training

Cyber Awareness Challenge training is required to be completed annually. If not completed, your account will be locked. Limited access may be granted to allow the user to complete their training. Once completed, it can take up to 48 hours before you regain full access to the network.

## Telecommunications Monitoring & Assessment Statement

"Do not transmit classified information over unsecured telecommunications systems. Official DoW telecommunications systems are subject to monitoring. **Using DoW telecommunications systems constitutes consent to monitoring.**"

## INCIDENT REPORTING AID

**Classification Justification:** _____

_____

**System Name (NIPR/SIPR):** _____

**Incident Type:** _____

**Date:** _____ **Time:** _____

**Location:** _____

**Description/Recovery Actions/Impact:** _____

_____

**Message Information**

**Date and Time Stamp:**_____

**From:**_____

**To:**_____

**Subject:**_____

**Classification\Name of Attachments:**_____

**Reported By**

**Name:** _____

**Phone:** _____

**Unit:** _____ **Rank:** _____

**Reported To:** _____ **Time:** _____

**Classify & handle "when filled" IAW DoDM5200.01V2_AFMAN16-1404V2**

**All incidents MUST be reported immediately!**

**TYNDALLAFBVA17-2, 4 May 2026, Supersede TYNDALLAFBVA33-101, 21 Mar 2016**

**OPR: 325 CS/SCXS**

**RELEASABILITY: There are no releasability restrictions on this publication.**

**POST THIS CARD AT ALL COMPUTER WORKSTATIONS**

(when filled in) CLASSIFICATION //_____//

# Tyndall Network Users Quick Reference Card

**REBOOT YOUR COMPUTER AT THE END OF THE DAY**

## Computer Support

Help Desk: DSN: 523-2666

## PHISHING ATTEMPT REPORTING PROCEDURES

*Unexpected ? Not digitally signed? Requesting information? Providing a link to click?*

| | |
|---|---|
| **STEP 1** | **NETWORK SECURITY FIRST!** Don't reply and never provide PASSWORD or CAC PIN to anyone! |
| **STEP 2** | **FORWARD PHISHING E-MAIL TO UNIT CL.** If Unit CL is not available or unknown, proceed to step 3. |
| **STEP 3** | **UNIT CL ADVISE YOUR WING CYBERSECURITY OFFICE AND UNIT CL FORWARD THE E-MAIL IF WARRANTED** |

*Messages in the Outlook Junk Folder already tagged as Phishing/Spam should be deleted. Reporting is not required.*

## COMPUTER VIRUS REPORTING PROCEDURES

| | |
|---|---|
| **STEP 1** | **STOP! DISCONNECT THE NETWORK CONNECTION FROM SYSTEM.** Discontinue ALL use. |
| **STEP 2** | **LEAVE THE SYSTEM POWERED UP.** Do not click on any prompts, close any windows, or shut down the system. |
| **STEP 3** | **DOCUMENT THE FOLLOWING:**<br>• Actions prior to virus<br>• If any error messages appeared<br>• Event date and time |
| **STEP 4** | **REPORT IMMEDIATELY!** Contact your Unit CL. If not available, contact the Wing Cybersecurity Office |

## CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES

*When a classified message is sent or received over an unclassified network*

| | |
|---|---|
| **STEP 1** | **STOP! DISCONNECT THE NETWORK CONNECTION** of the affected computer system(s) and/or printer(s). |
| **STEP 2** | **SECURE** affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance. |
| **STEP 3** | **REPORT INCIDENT IMMEDIATELY!** Contact your unit Security Manager. If by non-secure telephone say ONLY, "**I'd like to report a *possible* CMI**" and wait for personnel to assist. You can also report in person to your CL, Supervisor, and Wing ISSM. |

## Wing Cybersecurity Office

DSN: 523-2545 E-Mail: 325FW.cybersecurity@us.af.mil

**POST THIS CARD AT ALL COMPUTER WORKSTATIONS**