

# Privacy Rights How To

## SECURITY MANAGEMENT AWARENESS



## The Legal Requirements Of Privacy



- This training and awareness method is to be used by the U. S. Coast Guard Auxiliary for training members on Personal Identifiable Information (PII) rights and concerns within the organization.
- Privacy awareness is identified.
- Definitions are included.

**During a recent survey it was discovered that less than half the members knew that they could control their privacy information (PII) by Opt-Out on the website.**



# Definition

DHS defines personally identifiable information or PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII is any item, collection, or grouping of information about an individual that is maintained by an agency, including identifying information, education, financial transactions, medical history, and criminal or employment history. The following list provides examples of types of PII: Social Security Number, Date of Birth, Photographic Identifier (e.g., picture, photo image, X-ray, and video) Passport numbers, Place of birth, Mother's maiden name, Biometric information, such as fingerprints or retina scans, Medical information, Potentially sensitive employment information such as personnel ratings, disciplinary actions or results of background investigations, Criminal history, Any information that may stigmatize or adversely affect an individual.






# Reason for PII Protection & “How to”

The topic of member privacy (Privacy Communications Information) and (PII and Other Information) is being presented because of a recent request by a member of our organization to have a copy of a reference of organization policy that she could give to her supervisor. She was concerned that her Personally Identifiable Information (PII) was being made available for public viewing. In other words that there were no controls in place that would prevent someone from knowing her PII. The target group is all employees because it is a concern for everybody.

The Coast Guard Auxiliary’s policy on member privacy and PII is defined as;

- No personally identifiable information of a member is allowed to be displayed without their permission
- Documentation of such policies are in place and can be viewed online at <http://www.cgaux.org/privacy.php>
- The procedures can be read on how to file a complaint if necessary (handled through the appropriate Auxiliary chain of leadership and management)
- Person of contact (POC) are listed in the general menu and under each units website 
- The definition of PII can be read on the website along with the regulations <http://www.uscg.mil/auxiliary/publications/misc/alaux-008-11.asp>
- Controls are in place; on the members AuxDirectory website page at <https://auxofficer.cgaux.org/auxoff/>, the member can opt out or in on allowing his/her information to be displayed, the procedure for this is to log in to their AuxDirectory website page, scroll down to their unit and name, select the button to either opt in (allow) the display of their PII of email address, telephone and address or not allow.

It is the hope that this security and privacy training topic will bring the members to the awareness that there are policies and procedures in place already to protect and guard their PII.





# Member Concerns

- There has been a lot of concern about members addresses and other Personally Identifiable information (PII) being made visible.
- There is a way for the member to control this.
  - 1.) simply log into your AuxDirectory account with your member username and password. Drill down to members unit and name.  
<https://auxofficer.cgaux.org/auxoff/viewdetail.php>
  - 2.) In the section where it asks you to select "Display email; phone # ; etc.. Choose one or the other, Yes or No, to Opt In or Opt Out.  
**See below, the example on the next slide.**

**Please make sure your fellow members know this.**





# Personal Identifiable Information (PII)

- Members Opt In or Out Page
- Located in AuxDirectory

Work Phone:	
Offices:	FSO-CS, SO-CS, FSO-PB, BA-UCCA
Certifications:	BCCREW, IT, MDV, WS, FIRSTAID, CPR, TCO
Display Phone # on public websites	<input checked="" type="radio"/> YES <input type="radio"/> NO Instant Update
Display Email on public websites	<input checked="" type="radio"/> YES <input type="radio"/> NO Instant Update
Cell Phone is textable	<input checked="" type="radio"/> YES <input type="radio"/> NO Instant Update
Receive eMail Newsletters	<input checked="" type="radio"/> YES <input type="radio"/> NO Instant Update
Opt out of "I Want a VE" Program	<input type="radio"/> YES <input checked="" type="radio"/> NO Instant Update
<b>Skills Bank Detail</b>	
Occupation:	15-1142 Network and Computer Systems Administrators
Skills:	11-9039 Education Administrators, All Other 11-9199 Managers, All Other 15-1122 Information Security Analysts 15-1134 Web Developers 15-1142 Network and Computer Systems Administrators



# Education Requirements



- Sharing Sensitive PII: It is important to protect Sensitive PII at all times. Share it only with people who have an official “need to know.”
- Emailing to the wrong recipient or personal accounts: Never email Sensitive PII to a personal email account. If you need to work on Sensitive PII off site, use a DHS-approved portable electronic device.
- Preventing Compromised Mail: If documents can’t be scanned and encrypted or password-protected, mail them in an opaque envelope or container using First Class, Priority Mail, or a traceable commercial delivery service like UPS, the USPS, or FedEx.
- Accessing Sensitive PII while away from the office. The best method is to save the Sensitive PII on an encrypted, DHS-approved portable electronic device such as a laptop, Blackberry, CD, USB flash drive, or other removable media.
- Lost Media: Do not leave any portable electronic devices in a car. If it is stolen or lost, report it as a lost asset following your Auxiliary Privacy reporting procedures link on the website.
- Lost Hard Copies: Secure Sensitive PII in a locked desk drawer or file cabinet. When using Sensitive PII, keep it in an area where access is controlled and limited to persons with an official “need to know”. Avoid faxing Sensitive PII, if at all possible.
- Posting Sensitive PII to websites and shared drives: Do not post Sensitive PII on the Coast Guard Auxiliary intranet, the Internet (including social networking sites), shared drives, or multi-access calendars that can be accessed by individuals who do not have an official “need to know.”





# Privacy at Coast Guard Auxiliary: Protecting Personal Information

You Can Promote Privacy at Coast Guard Auxiliary.

To promote privacy at Coast Guard Auxiliary, it is important to:

1. Partner with your Auxiliary Privacy Office when posting or planning new or updating existing programs, systems, technologies or rule-makings to ensure compliance with privacy laws.
2. Follow the procedures outlined in the Handbook for Safeguarding Sensitive PII at Coast Guard Auxiliary.
3. Report all suspected or confirmed privacy incidents immediately. (Auxiliary websites will have a Report link on the main menu page)

And when you work with Sensitive PII, be sure to consult the two Job Aids as well as the other resources listed on the Privacy Resources page on the next slide.





# Resources

- [How to Safeguard PII Job Aid](#)
- [Telework Best Practices Job Aid](#)
- [Handbook for Safeguarding Sensitive PII at DHS](#)
- [How to Restrict Access on a Shared Drive](#)
- Privacy Office website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy)

U.S. Government Privacy Laws Certification

[https://privacyassociation.org/media/pdf/certification/CIPP\\_G\\_BoK.pdf](https://privacyassociation.org/media/pdf/certification/CIPP_G_BoK.pdf)

For privacy concerns, consult your Coast Guard Auxiliary Privacy Officer or Privacy Point of Contact.







# Personal Information Devices

Federal law requires anyone with a personal portable electronic device such as tablet, smart phone or laptop computer that could be used to store sensitive information be protected with password and security software in case of being lost or stolen.





# Potential Consequences of Not Protecting PII

For the Coast Guard Auxiliary:

- Loss of public trust
- Increased Congressional oversight
- Loss of funding

For the victim:

- Identity theft
- Loss of benefits
- Embarrassment

For the person causing the privacy incident:

- Counseling and training
- Loss of employment
- Civil & criminal penalties





# Report Privacy Incidents

If you:

- Lose, allow, or witness unauthorized access to Sensitive PII.
- Unintentionally release Sensitive PII.
- Misuse Sensitive PII.
- Cause files or systems to become compromised.
- Know or suspect that any of the above has occurred.

You **MUST** report the privacy incident, either suspected or confirmed, immediately to your supervisor, Auxiliary help desk, privacy officer, or privacy point of contact. (A link to a reporting PDF form will be added soon to the website)





# More Information Links

**Mandated Training Requirements: ALAUX 037/10**

**<http://www.uscg.mil/auxiliary/publications/misc/alaux-008-11.asp>**

**AUXILIARY LEARNING MANAGEMENT SYSTEM (AUXLMS)  
BENEFITS, REQUIREMENTS, AND IMPACTS ON AUXILIARY MANDATED TRAINING**

**<https://www.uscg.mil/auxiliary/training/auxlms.asp>**

**PRIVACY INCIDENT RESPONSE, NOTIFICATION, AND REPORTING**

**[www.uscg.mil/directives/ci/5000-5999/CI\\_5260\\_5.pdf](http://www.uscg.mil/directives/ci/5000-5999/CI_5260_5.pdf)**

**PRIVACY ACT STATEMENT**

**[www.uscg.mil/foia/healy/Number%20101-218/num\\_115.pdf](http://www.uscg.mil/foia/healy/Number%20101-218/num_115.pdf)**

**Freedom of Information (FOIA) and Privacy Act (PA) Requests**

**[www.uscg.mil/d9/D9Legal/FOIA&PrivacyAct.asp](http://www.uscg.mil/d9/D9Legal/FOIA&PrivacyAct.asp)**

**Website Privacy Policy - U.S. Coast Guard Navigation Center**

**[navcen.uscg.gov/?pageName=Privacy](http://navcen.uscg.gov/?pageName=Privacy)**





# End of Privacy Rights and Concerns Module

By Ronald Dell

*Guarding the Guardians/Protecting the Protectors*



**Privacy Awareness Training**