



**Health Services**  
LOS ANGELES COUNTY

## POLICIES AND PROCEDURES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO:** 935.20

---

**PURPOSE:**

To ensure the entire Department of Health Services (DHS) workforce follow acceptable use of County information technology resources within the department.

**POLICY:**

Each DHS workforce member is required to adhere to and management is expected to strictly enforce all policies and procedures with respect to the proper use of County information technology resources in accordance with DHS Policy No. 361.1, DHS Privacy and Security Compliance Program, the County Fiscal Manual, and other County and DHS information technology use policies and procedures.

All workforce members are required to sign acknowledgment of the receipt and review of the County and DHS' Acceptable Use policy (as noted below). DHS Human Resources must ensure that each new hire or transferred County workforce member receives and signs the following documents during in-processing

- 1) *County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data (County Acceptable Use Agreement)* and,
- 2) Acknowledgment of this policy

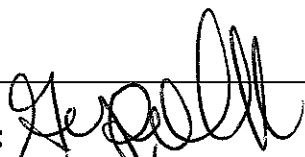
Managers/supervisors must review both documents and have them signed and completed by each County workforce member during the annual performance evaluation process.

Each Non-County workforce member shall receive and acknowledge the "DHS Comprehensive Policy Statement" in accordance with the non-County workforce member in-processing procedures. The "DHS Comprehensive Policy Statement" must also be provided to and acknowledged by the non-County workforce member in conjunction with their annual performance review process.

---

**APPROVED BY:**

**REVIEW DATES:**

  
8/14/12

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

DHS System Managers/Owners will ensure that all workforce members with access to County information technology resources have signed the agreement and acknowledgment prior to providing access.

## **I. RESPONSIBILITY**

Access to County information technology resources and accounts is a privilege granted to workforce members based on their job duties and may be modified or revoked at any time. Each workforce member is responsible for the protection of DHS' County information technology resources. Workforce members must protect all Information contained in the technology resources as required by local, state and federal laws and regulations. Each workforce member must sign and abide by the County Acceptable Use Agreement and the provisions of this policy.

County workforce members will be required to sign the County Acceptable Use Agreement and the acknowledgment at the time of new hire or transfer into DHS and annually as part of the performance evaluation process. Non-County workforce members will be required to acknowledge the County Acceptable Use Agreement and this policy by signing the "DHS Comprehensive Policy Statement" during the in-processing procedure and in conjunction with their annual performance review.

The completed acknowledgment forms must be filed in the workforce member's personnel folder. Acknowledgments from the "DHS Comprehensive Policy Statement" will be filed in the non-County workforce member's Human Resources file.

Violation of the County Acceptable Use Agreement or this policy may result in disciplinary action, up to and including, discharge and possible civil and/or criminal liability.

Non-County workforce members found to be in violation of the County Acceptable Use Agreement or this policy may be released from assignment and recorded as a "do not send" in the DHS "Do Not Send" Database.

The County information technology resources are the property of the County and are to be used for authorized business purposes only.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 2 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

## II. WORKFORCE MEMBER PRIVACY

Workforce members have no expectation of privacy with respect to their use of the County information system assets, because at any time DHS may log, review, or monitor any data created, stored, accessed, sent, or received. DHS has, and will exercise, the right to monitor any information stored on a workstation, server or other storage device; monitor any data or information transmitted through the DHS network; and/or monitor sites visited on the DHS Intranet, Internet, chat groups, newsgroups, material downloaded or uploaded from the Internet, and e-mail sent and received by workforce members. Activities, communications, or computer usage not related to County business are likely to be monitored. DHS may use manual or automated means to monitor use of its County information technology resources.

A supervisor/manager may request to review the system activities of a subordinate if misuse of DHS system resources is suspected. If evidence of misuse of DHS system resources is identified, the supervisor/manager must contact the DHS Audit & Compliance Division to determine appropriate actions. The DHS Audit & Compliance Division may also be required to contact the Auditor-Controller's Office of County Investigations.

Violations involving non-County workforce members shall be referred to the Facility Liaison/Contract Monitor for appropriate action.

Use of passwords to gain access to County information technology resources or to encode particular files or messages does not imply any expectation of privacy in the material created or received. The requirement for use of passwords is based on DHS' obligation to properly administer information technology resources to ensure the confidentiality, integrity and availability of Information. Workforce members are required to authenticate with a unique Employee/Workforce member ID so that all access may be auditable.

## III. PROHIBITED ACTIVITIES

A. Prohibited Uses: Workforce members are prohibited from using County information technology resources for any of the following activities:

1. Engaging in unlawful or malicious activities.
- 

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 3 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

2. Sending, receiving or accessing pornographic materials.
3. Engaging in abusive, threatening, profane, racist, sexist or otherwise objectionable language.
4. Misrepresenting oneself or the County.
5. Misrepresenting a personal opinion as an official County position.
6. Defeating or attempting to defeat security restrictions on County systems or applications.
7. Engaging in personal or commercial activities for profit.
8. Sending any non-work related messages.
9. Broadcasting unsolicited, non-work related messages (spamming).
10. Intentionally disseminating any destructive program (e.g., viruses).
11. Playing games or accessing non-business related applications, or social networking sites.
12. Creating unnecessary or unauthorized network traffic that interferes with the efficient use of County information technology resources (e.g., spending excessive amounts of time on the Internet, engaging in online chat groups, listening to online radio stations, online shopping).
13. Attempting to view and/or use another person's accounts, computer files, program, or data without authorization.
14. Using County information technology resources to gain unauthorized access to DHS or other systems.
15. Using unauthorized wired or wireless connections to DHS networks;
16. Copying, downloading, storing, sharing, installing or distributing movies, music, and other materials currently protected by copyright, except as clearly permitted by licensing agreements or fair use laws.
17. Using County information technology resources to commit acts that violate state, federal and international laws, including but not limited to laws governing intellectual property.
18. Participating in activities that may reasonably be construed as a violation of National/Homeland security.
19. Posting scams such as pyramid schemes and make-money-quick schemes.
20. Posting or transmitting private, proprietary, or confidential information, including patient information, to unauthorized persons, or without authorization.
21. Downloading confidential or patient information or data onto a mobile storage device without authorization from the Facility CIO/designee.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 4 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

22. Using Online Web-based Document Sharing Services (e.g., Google Docs, Microsoft Office Live, Open-Office) to store or share DHS data.
  23. Viewing, accessing, using or disclosing confidential or patient information or data if not authorized as part of the workforce member's job duties.
- B. Misuse of software: Workforce members must not engage in software copyright infringements. Workforce members are prohibited from conducting the following activities without proper licensing and prior written authorization by the Facility CIO/designee:
1. Copying County-owned software onto their home computers.
  2. Providing copies of County-owned software to independent contractors, clients or any other third-party person.
  3. Installing software on any DHS workstation (e.g., desktops, personal computers, mobile devices, and laptop) or server, unless authorized by their supervisors and IT management.
  4. Downloading software from the Internet or other online server to DHS workstations or servers.
  5. Modifying, revising, transforming, recasting or adapting County-owned software.
  6. Reverse-engineering, disassembling or decompiling County-owned software.

## IV. PASSWORDS

Workforce members are responsible for safeguarding their passwords for access to the County information technology resources. Workforce members are responsible for all transactions made using their passwords. Workforce members may not provide their password or use their password to provide access to another Workforce member; or access the County information technology resource with another Workforce member's password or account. Some systems have a universal access password with a secondary password neither of which shall be shared with workforce members who are not authorized to utilize the system. Workforce members should be aware that leaving a computer unattended for a brief time, even 30 seconds, may give an unauthorized user enough time to access the system using the previous user's access.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 5 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

## V. SECURITY

### A. County information technology resources

Workforce members are responsible for ensuring that the use of outside computers and networks, such as the Internet, do not compromise the security of County information technology resources. This responsibility includes taking reasonable precautions to prevent intruders from accessing County information technology resources.

### B. Malicious software

Malicious software can cause substantial damage or inconvenience to County information technology resources. Workforce members are responsible for taking reasonable precautions to ensure that they do not introduce malicious software into County information technology resources. Workforce members must not bypass or disable County malicious software protections. Workforce members must only use or distribute storage media or e-mail (including attachments) known to the workforce member to be free from malicious software.

Any workforce member who telecommutes or is granted remote access must utilize equipment that contains current County-approved anti-virus software and must adhere to County hardware/software protection standards and procedures that are defined by the County and the authorizing Department.

DHS restricts access to the Internet or any other network via modem, cellular wireless, or other telecommunication services. No workforce member may employ any external inbound or outbound connections to DHS network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Each workforce member is responsible for notifying the Department's Help Desk or the Department Security Contact as soon as a device is suspected of being compromised by a virus.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 6 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

## VI. E-MAIL

Access to County e-mail services is a privilege that may be wholly or partially restricted without prior notice and without consent of the workforce member. E-mail messages are the property of the County and subject to review by authorized County personnel.

E-mail messages are legal documents. Statements must not be made on e-mail that would not be appropriate in a formal memo. Workforce members must endeavor to make each electronic communication truthful and accurate. Workforce members are to delete e-mail messages routinely in accordance with both the DHS and County E-mail policies.

Protected Health Information (PHI) and other confidential and/or sensitive information can only be sent or received if it is encrypted or safeguarded in accordance with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

Access to Internet-based e-mail sites (e.g., Yahoo Mail, Google Mail, Hotmail, etc.) is not permitted. Exceptions to this policy must be based upon requirements to perform job-related activities and be approved by DHS management.

### Default E-Mail Retention Period

DHS e-mail systems will be configured to **automatically delete** messages greater than **three years** on active e-mail servers. This auto-delete policy applies to messages within all folders (inbox folders, sent file folders, draft file folders, etc.) stored on active e-mail servers. DHS will have three levels of e-mail users. (Level 1 is 3 years, Level 2 is 5 years, and Level 3 is 7 years of retention time)

All DHS e-mail system users are expected to:

1. Regularly check for new messages;
  2. Delete **transitory** messages as quickly as possible.
    - a. Specially defined groups will have a maximum of either a five or seven year retention period.
    - b. Specially defined groups may consist of members from Audit and Compliance, Risk Management, Human Resources, Finance, and facility CEO's.
- 

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 7 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

- c. Facility CEO's and Executive Management from defined groups will determine which individuals will be allowed a five or seven year retention period.
- d. No Personal Storage Table, (PST) files will be allowed or used by DHS e-mail users.
- e. E-mail is not to be used for the storage of patient/protected health information of any kind, nor is it to be used as a document storage system.

## **VII. USE OF THE INTERNET**

Use of the Internet must be in accordance with DHS and County Internet and privacy policies.

All DHS Internet activities are monitored and audited by DHS Security Operations and Compliance Divisions.

Unauthorized non-County business Instant Messaging and Streaming Media are strictly prohibited.

Workforce members must not allow another workforce member to access the Internet using their authorized account.

DHS is not responsible for material viewed or downloaded by workforce members from the Internet. The Internet is a worldwide public network that is uncensored and contains sites that may be considered offensive. Workforce members accessing the Internet do so at their own risk and DHS shall not be liable for inadvertent exposure to any offensive materials.

Internet access is provided to the workforce member at the discretion of each DHS Facility.

## **VIII. INFORMATION TECHNOLOGY USER ACCOUNT MANAGEMENT**

When a workforce member leaves the County service, the supervisor must inform the local service desk to have the workforce member's Information Technology (IT) user accounts deactivated immediately. All IT accounts that have been deactivated for 60 days or more will be deleted. The workforce member's supervisor will be

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 8 OF 14**



# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

contacted for approval to delete the accounts. In cases where the supervisor failed to inform the local service desk, Human Resources records will be used to disable accounts that have not been active in the last 60 days. All IT accounts that have been inactive for 60 days or more will be deleted.

Each Facility's Information Technology Department shall adhere to this minimum standard/guideline.

Each Facility's Information Technology Department shall develop and implement procedures to ensure compliancy.

## **IX. RECORDABLE MOBILE DEVICES AND REMOVABLE MEDIA**

Workforce members must manage and control all recordable mobile devices and removable media that contain PHI or other confidential information. These devices include PDA's, USB flash drives, personal cell phones, cameras, removable hard disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

The use of recordable mobile devices and removable media must be pre-approved and registered for use by the Facility CIO/designee in accordance with DHS Policy No. 935.11, Workstation Use and Security : Access and Use of Mobile Devices and DHS Policy No. 935.13 Device and Media Controls: Accountability.

## **X. REMOTE ACCESS SERVICES**

No workforce member may employ any remote inbound or outbound connections to DHS network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Unauthorized Remote Access Services (e.g., LogMeIn, GoToMyPC) are strictly prohibited.

Any workforce member who is granted remote access to the DHS network must utilize the approved DHS Information Security method for remote access. VPN is the DHS approved remote access solution until further notice.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 9 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

Dial-up, DSL, modem etc. are strictly prohibited.

At no time should any workforce member share their remote access privileges with anyone, including other workforce members or family members.

## **DEFINITIONS:**

**INFORMATION TECHNOLOGY RESOURCES/ASSETS** Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

**INFORMATION TECHNOLOGY USER ACCOUNTS** An authorized user account (i.e., E-mail, Internet, Network File Share, Health Information System, etc.) provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account.

**WORKFORCE MEMBER** Employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

**MALICIOUS SOFTWARE** The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms.

**PERSONAL STORAGE TABLE** A file that stores e-mail messages, calendar events and contact information used in applications such as Microsoft Outlook.

**REMOTE ACCESS SERVICE** A service that supports connecting a PC from a location outside of the DHS network (e.g. home) to the DHS network or vice versa.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00 DHS Information Technology and Security Policy.

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 10 OF 14**

# DEPARTMENT OF HEALTH SERVICES COUNTY OF LOS ANGELES

**SUBJECT:** ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY  
RESOURCES

**POLICY NO.:** 935.20

---

**AUTHORITY:**

Board of Supervisors Policies:

- 6.101, Use of County Information Technology Resources
- 6.102, Countywide Antivirus Security Policy
- 6.104, Use of Electronic Mail (E-mail) by County Employees
- 6.105, Internet Usage Policy

**CROSS  
REFERENCES:**

DHS Policy Nos.:

- 361.1, DHS Privacy and Security Compliance Program
- 361.23, Safeguards for Protected Health Information (PHI)
- 935.00, DHS Information Technology and Security Policy
- 935.11, Workstation Use and Security
- 935.13, Device and Media Controls

---

**EFFECTIVE DATE:** August 15, 2012

**SUPERSEDES:** September 1, 2009

**PAGE 11 OF 14**

**COUNTY OF LOS ANGELES  
AGREEMENT FOR ACCEPTABLE USE AND  
CONFIDENTIALITY OF  
COUNTY'S INFORMATION TECHNOLOGY ASSETS,  
COMPUTERS, NETWORKS, SYSTEMS AND DATA**

As a Los Angeles County, employee, contractor, vendor, or other authorized employee of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As an user of County's IT assets, I agree to the following:

1. Computer Crimes: I am aware of California Penal Code 502(c) – Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.
2. Security Access Controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.
3. Approved Business Purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.
4. Online Web-based Document Sharing Services  
I will not use Online Web-based Document Sharing Services to collaborate with workforce members; to store and/or share DHS owned data.
5. Unauthorized Application or Software  
I will not download, install, or use any non-DHS approved application or software, such as Instant Messaging, Streaming Media, and Remote Access Services (e.g., LogMeIn, GoToMyPC).
6. Confidentiality: I will **not view, access, use or disclose** any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.
7. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County computers, servers and other computing devices I am responsible for.
8. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.

9. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.
10. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County and DHS e-mail use policy and use proper business etiquette when communicating over e-mail systems.
11. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.
12. Passwords: **I understand that I am responsible for safeguarding my passwords for access to County information technology resources and am responsible for all transactions made using my password. I will not share my passwords or provide access to another individual using my password.**
12. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, and cancellation of contracts or both civil and criminal penalties.

CALIFORNIA PENAL CODE 502(c)  
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website [www.leginfo.ca.gov/](http://www.leginfo.ca.gov/).

502. (c) Any person who commits any of the following acts is guilty of a public offense:
- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
  - (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
  - (3) Knowingly and without permission uses or causes to be used computer services.

- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system or computer network.

**ACKNOWLEDGMENT:**

I acknowledge that I have received and read the Department of Health Services' Policy No. 935.20, DHS Acceptable Use Policy for County Information Technology Resources and the County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data. I agree to abide by the provisions of the policy and the agreement. If I fail to comply with the policy and agreement, I will be subject to disciplinary action, up to and including discharge or release from assignment.

If I have any questions concerning the policy or agreement, I will discuss them with my supervisor.

Name (print):	Employee/Contractor ID No.:	Date:
Signature:	Job Title:	Department No.:
Supervisor Name (print)	Supervisor Signature:	Date:

DHS Policy No. 935.20 Rev 7/6/12