

**Employee
INFORMATION SECURITY
Handbook**



**Department of Health and Human Resources
2003**

TABLE OF CONTENTS

	Page
Why this handbook?	1
What will I learn from this handbook?	1
What is Information Security?	1
Why is INFOSEC important?	2
Role and Duties of the ISO	2-3
Potential Dangers to Information Systems	3-4
Threats, Vulnerabilities and Risks	3-4
Social Engineering	4
IT Policies	4-5
Policy Violations	5
Employee Responsibilities	5-8
Passwords	5-6
Unattended Workstations	6
Desktop Audits	6
Internet Use	6-7
Intranet Use	7
E-mail Security	7
Physical Security	8
Summary	8
Glossary	9-10
Contact Us	11

Why this handbook?

This handbook has been designed to provide awareness to you about Information Security and to identify supporting reference materials to allow you to properly protect agency information.

What will I learn from this handbook?

By reading this handbook, you will have a better understanding of the following:

1. What Information Security is and why it is important to you;
2. Why threats, vulnerabilities, and risks are significant to Information Security;
3. What IT policies are, and what they mean to you;
4. Who the Information Security Officer (ISO) and the Information Security Liaisons (ISL) are, and what their responsibilities are in relation to Information Security issues; and
5. What your responsibilities are as a DHHR employee.



What is Information Security?

Information Security is about preserving an organization's overall information asset in its intended condition and ensuring its integrity, privacy, and availability to information users.

The ultimate goal of raising Information Security awareness among our staff is to accomplish the three universal conditions of secure information: **Confidentiality, Integrity, and Availability.**

Confidentiality is protecting information from unauthorized disclosure.

Integrity is maintaining information in its intended form, free from unauthorized or accidental alteration.



Availability is the unimpaired access to information or information systems. It requires that the information or processing is accessible on demand, and comes to the user without significant delays.

Why is INFOSEC (Information Security) Important?



Information is a valuable asset and must be protected in order to minimize information leaks, unintended alterations, or losses.

As information grows in volume, complexity, and criticality, and as access to data broadens, it becomes both increasingly valuable and vulnerable.

More people are able to access data than ever before, which exposes that data to corruption, destruction, theft, malice, and error.

Information Security is dependent upon a wide range of factors including organizational, technical, and human factors.

No matter how sophisticated and expensive an information security effort may be, in the final analysis it's the human beings involved in that effort who determine its effectiveness.

An effective Information Security program is essential for the DHHR to protect its information assets. It is each employee's responsibility to help make sure that the Department's data remains intact.

The absence of adequate Information Security within the DHHR can result in many kinds of wrongs to clients, financial loss, legal liability, and the misuse of information, as well as the loss of State assets, confidentiality, and credibility.

Role and Duties of the Information Security Officer



The Information Security Officer leads the overall Information Security program for the Department.

The ISO defines, implements, promotes, and maintains an appropriate Information Security plan for the Department.

The ISO investigates and resolves security violations, and involves Department management in the issues surrounding Information Security.

The ISO's duties include monitoring Information Security activities and contingency plans, as well as participating in the planning and adoption of new technologies.

DHHR management has appointed ISL's (Information Security Liaisons) as members of the INFOSEC Team. They will maintain a heightened sense of security awareness throughout the Department and in DHHR offices throughout the state.

One duty of the ISL is performing ad hoc desk audits. During these audits, the ISL will be looking for passwords left in plain view, as well as workstations left logged-on and unattended.

Occasionally, ISL's will be asked to perform desk audits outside of normal work hours. They, along with a local manager or designated representative, will look for confidential material left in plain view, passwords left under keyboards, mouse pads or taped to surfaces, or logged-on workstations, etc.

The ISL should be considered a resource and point of contact for any security awareness questions or concerns.

Potential Dangers to Information Systems

Threats, Vulnerabilities, and Risks

Three key terms used to assess and implement improvements in an organization's Information Security plan are **threats**, **vulnerabilities**, and **risks**.



Threats are events or activities that have the potential to cause damage to information or information systems.

Vulnerabilities are weaknesses that may be used by a threat in a way that would lead to damage to the information or information systems.

Risks are the costs and the probabilities of a loss of information or other assets.

You should realize that threats do not always appear to be risky. *User mistakes* are threats, even though they may not be malicious or intentional. Also, vulnerabilities are not always obvious. If someone claiming to be "from the Help Desk" calls you and asks you for your user id and password, are you a vulnerability?

If you give anyone your password, you are a vulnerability!

Common sense will go a long way toward reducing vulnerabilities, and therefore, reducing risks. As you read this information and grasp the concepts of Information Security, you will become less of a vulnerability to the organization, while helping build resistance to the threats that jeopardize our information assets and systems.

Social Engineering



Social Engineering is the act of deception, and misrepresentation of identity or authorization, to gain information or physical access. This can result in the loss of confidentiality, integrity, and availability of information, or the loss of property through outright theft.

The following are examples of Social Engineering that have been successfully used to gain physical access or information and to perform acts of theft:

(1) gaining access to a building by "making friends" with smokers at a doorway and following them into a building which is normally restricted (also called tailgating);

(2) approaching a doorway carrying a large box and taking advantage of an unsuspecting person's willingness to hold the door open without questioning the intruder's right to be inside;



(3) approaching a doorway while talking on a cell phone and taking advantage of the politeness of an authorized person who will hold the door, but will not interrupt the conversation to determine this person's identity and authorization to enter the building;



(4) calling and claiming to be "from the MIS Help Desk" and asking for your ID and password to allow you to be kept in the system after an upgrade has been performed; or

(5) mailing a CD or diskette to a user, possibly one with an unusual shape or label that may entice the recipient to put it in the CD drive of their computer. This CD can contain code that automatically loads to the PC and initiates a contact to a hacker's computer on the outside of the organization through the firewall.

The externally located perpetrator can then access the system to gain control and compromise information or information systems resources.

IT (Information Technology) Policies



DHHR IT Policies are the foundation of Information Security within our organization. They focus on requirements for the security and well-being of information assets and resources.

IT Policies are written statements, endorsed by upper management, which define the type and scope of controls required for the use of information technology products, processing, and data. Policies come directly from standards of conduct, and often emphasize matters of common sense and common courtesy that apply to the use of any shared resource.

IT Policies lay the groundwork for developing and implementing secure practices within an organization, and they define the rules that must be followed.

DHHR IT Policies can be found at the following web address:
<http://www.wvdhhr.org/mis/IT/index.htm>

Policy Violations



When a policy is violated, disciplinary actions may be taken. These actions will be consistent across the Department, and will conform with enforcement rules spelled out in current IT policies and procedures.

When there is suspicion that an employee has violated an IT policy or the law (Chapter 61, Article 3C, WV Computer Crime and Abuse Act), an investigation of computer activity may be launched.

If you suspect that a security or computer violation exists, contact a manager or the Information Security contacts found at the end of this booklet.

Employee Responsibilities

All DHHR employees are responsible for protecting their own information assets and are accountable for their actions relating to information resources. You must always be aware of possible threats and vulnerabilities to the DHHR's information systems. The following sections focus on some of the most important ways you can support the INFOSEC mission.



Passwords



Using strong passwords is an important aspect of Information Security. You must always create passwords that are difficult to guess or "crack". To achieve this goal, use passwords that do not contain common words, linked common words, and/or words with numbers or punctuation at the beginning or end.

An example of how to create a strong password is to use the first letter of each word in a personal phrase while incorporating numbers and/or special characters.

For example, M2fsRb&b = My 2 favorite sports R baseball & basketball.

Passwords must **NEVER** be shared with any individual for any reason. (see section on Threats, Vulnerabilities and Risks). You are responsible for all activity that occurs on your computer while you are logged-on to it .

Sharing a password can compromise the security of the entire system. It is also a violation of OP-012 and, in certain circumstances, the Computer Crimes and Abuse Act, [WV Code 61-3C-10](#).

Unattended Workstations

Both IT Policies 0501 and 0511 state that employees must always lock or log off PC's when leaving workstations. This is for your protection, as well as the protection of DHHR systems.

Leaving your workstation unattended could result in an unauthorized person assuming your online identity.

Desktop Audits



You should be aware that ISL's, accompanied by a manager or designee, will be conducting desktop audits both during the day and outside of normal business hours. Make sure any confidential information and/or passwords are out of plain sight and in a locked drawer or file cabinet. Be certain your PC is logged-off and secured whenever you leave your work area.

ISL's will also be looking for inappropriate applications or any unnecessary privileges, such as chat programs or streaming audio and video.

Appendix B of IT Policy 0501 states that "any use in relation to installing MP3 files or participating in chain letters or chat programs" is prohibited.

Internet Use



Internet access is for the purpose of increasing productivity. Surfing the net, or wandering away from your business objective is not a productive or acceptable use of this tool. This misuse can connect you to web sites that may contain programs that appear harmless, but could cause damage to DHHR systems.

Because it is plain text, most information transmitted over the Internet is subject to interception, reading, and copying by other people. Encryption, which scrambles information during transmission, reduces this vulnerability.

Physical Security



In an effort to reduce risks to IT assets, the physical security of DHHR computing resources must be ensured.

Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data.

For example, server rooms must remain safe, secure, and inaccessible to unauthorized individuals, and storage cabinets containing critical business records must always be kept locked and secured.

Be aware of those areas with restricted access. Make sure that individuals entering these areas are displaying proper DHHR identification.

Tailgating is a term used in the context of Physical Security to mean, “gaining access to a restricted space by following an authorized individual through a doorway.”

Be aware of people who follow you into restricted building areas who do not display proper employee identification. If they do not, you should tell them to report to the Security Station through a public access door.

Even if you think you recognize someone as an employee, you CANNOT simply let them in the door. You have no way of knowing if they have been recently suspended or terminated.

Proper security must also be maintained around outside doors and windows to prevent unauthorized entry, which could cause damage to DHHR assets. For example, make sure doors and/or windows are not propped open with cardboard or other obstructions. Report any deficiencies or non-secure conditions to management immediately.

Summary

This handbook was developed to help you understand not only what Information Security is, but why it is important to all DHHR employees. A discussion of threats and vulnerabilities, as well as risks to Information Security, was provided.

IT Policies have been presented as the framework of Information Security for the Department, and a link was given to the website where all DHHR IT Policies are located. The importance of not sharing passwords has been emphasized, and the roles and duties for both the ISO and ISL's have been presented.

Perhaps the most important information contained within this handbook was the discussion of your responsibilities as a DHHR employee. If you have not carefully read and understood this handbook in its entirety, then you are already behind in meeting your obligation.

Glossary

Availability - the unimpaired access to information or information systems.

Confidentiality - the protection of information from unauthorized disclosure.

Desk Audits - Inspections conducted to make sure that confidential information or passwords are out of plain sight and workstations are not left unattended.

Encryption - The process of encoding data so that it is inaccessible to unauthorized users.

Firewall - A hardware device or software that isolates a system from other systems on a Local Area Network (LAN) or Wide Area Network (WAN).

Hacker - A person who breaks into a computer system to view, alter, or steal restricted data and programs.

Information Assets - The comprehensive group of valued and protected information and information processing. This includes, but is not limited to: documents, data, and data processing and storage hardware and software.

Information Security - The awareness of, and conformance with, information security policies and procedures.

Information Security Liaison (ISL) - Individuals appointed by DHHR management to maintain a heightened sense of security awareness and compliance with information security policies and procedures.

Information Security Officer - An Individual who maintains and promotes compliance with the DHHR Information Security plan.

Information Technology (IT) - The technology involved with the transformation and storage of information, especially that used for the development, installation, implementation, and management of information systems and applications within the DHHR.

Internet - A web of networks that interconnects millions of supercomputers, mainframes, workstations, personal computers, laptops, and hand-held computers.

Integrity - Information that is free from any unintended alteration by the information asset owner.

Intranet - A private network that provides services similar to those found on the Internet, yet is contained completely within an enterprise's systems environment.

Local Area Network (LAN) - A network that links together computers and peripherals within a limited area, such as a building or group of buildings.

Risk - The costs and probabilities of loss of information or other assets.

Social Engineering - The act of deception and/or misrepresentation of identity to gain information or physical access.

Tailgating - With regard to physical security, this relates to gaining access to a restricted space by following an authorized individual through a doorway.

Threats - Unintentional or accidental events or activities that may cause damage to information or information systems.

Vulnerability - A weakness that may be used by a threat that could lead to damage to information or information systems.

Wide Area Network (WAN) - A network that uses such devices as telephone lines, satellite dishes, or radio waves to span a larger geographic area than can be covered by a LAN.

Contact Us



Your Manager	
Information Security Officer	
Jim Richards	558-7816
jarichards@wvdhhr.org	
Deputy Information Security Officer	
Jim Weathersbee	558-9193
jimweathersbee@wvdhhr.org	
MIS Help Desk	558-9999

ITOPS

Information Technology Operations, Policy, and Security

350 Capitol Street, Room 313

Charleston, WV 25301-3713

A division of Management Information Services

Department of Health and Human Resources

<http://www.wvdhhr.org>

© ITOPS 2003