

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 19

JUNE 2007

Resources

Privacy Program
(503) 945-5780

Information Security
(503) 945-6812

**Information Security/
Privacy Web site**
[www.oregon.gov/DHS/
admin/infosec/](http://www.oregon.gov/DHS/admin/infosec/)

Privacy Help Email
PrivacyHelp, DHS

Information Security Email
SECURITY, DHSINFO

Privacy Policies
[www.dhs.state.or.us/policy/
admin/privacypolicy.htm](http://www.dhs.state.or.us/policy/admin/privacypolicy.htm)

Information Security Policies
[www.dhs.state.or.us/policy/
admin/infosecuritylist.htm](http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm)

*Send requests for
future Privacy/Security
Update topics to:
dhs.privacyhelp@state.or.us*



Groupwise Email Security

QUESTION: Can we send confidential, sensitive information through our GroupWise email system?

ANSWER: Yes, with some considerations.

Kyle Miller, DHS Information Security Officer, states that email sent within the GroupWise system is secure, but although it is secure, it is still vulnerable to being misdirected and thus accessed by someone who does not have a need to know the information.

A policy to address the use of email for confidential information is being developed but it will not be finalized until encryption software is implemented at the State Data Center. The software will provide security for email going outside of the GroupWise system. DHS is working with SDC to ensure that the secure email system has the same characteristics as the current email system and hopes to have it implemented sometime during the summer of 2007.

Email containing confidential information sent outside of the GroupWise system is NOT secure. There is no current policy addressing this, but we have policies directing us to apply reasonable safeguards to protect confidential information. Until the email policy is completed and secure email is implemented at SDC, ISO recommends:

1. Apply reasonable safeguards to all confidential communication, and use only the minimum amount of information needed to complete the task.
2. Be aware that email sent outside the GroupWise system is NOT secure.
3. Check and recheck email addresses to prevent the confidential information from being misdirected.
4. Do not use client names or other individually identifiable information in the subject line.
5. Where business processes are totally dependent on the use of email, proceed as usual until further notice. Apply reasonable safeguards to email and all other methods of confidential communication.

For additional questions, contact the Information Security Office at 503-945-6812 or dhsinfo.security@state.or.us

What Is Incident Management?

Incident Management, also known as “Incident Response” in the DHS Information Security Office (ISO) world, captures both privacy and information security incidents. ISO is responsible for receiving, reviewing, and responding to privacy/information security incidents, with involvement from department representatives in the resolution process.

Why is it important that incidents are reported?

When incidents are reported, data is captured and statistics arise that show us trends, areas of concerns and processes that need improving. An example of this is GroupWise email groups. Using statistical information, ISO worked with OIS and other business units to address flaws in the use and assignment of GroupWise email groups.

Appropriate use of GroupWise email:

A computer-based training module was developed and implemented to help staff understand and use GroupWise Email appropriately. These efforts significantly reduced misdirected E-mails and the disclosure of sensitive information by 80% (based on 2005 and 2006 PSIRP data).

Use of regular mail:

A high number of incidents involving regular mail were recorded as a result; the Information Security Office convened a task group to examine the incidents of inadequately addressed and poorly packaged mail that contained confidential, sensitive information.

The goal of the task group is to design an effective process for mailing and shuttling confidential, sensitive information, and to plan an awareness and education program so that the new process will be communicated to all program areas and all branch offices.

Remember that DHS information security and privacy is everyone's responsibility and you can make a difference!

Problematic Spam

‘Spam’ is the term used for unsolicited and unwanted electronic messaging. Email is now a significant communication channel and anything affecting its functionality is of concern. Spam is a growing problem, even at DHS.

“SPAM” cont. next page...

Privacy Contacts

Privacy Officer

Jane Alm, (503) 947-5255

Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Gloria Anderson

CAF/Pro. & Policy, (503) 945-5700

Ronald Barcikowski

CAF/OVRS, (503) 945-6734

Donna Weaver

SPD/Field Services, (503) 945-5977

Marilee Bell

SPD/DD, (503) 947-5262

Diane Duncan

OMHAS, (503) 945-6083

Steve Modesitt

Public Health, (971) 673-1293

Joni DeTrant

State Hospitals, (503) 945-2981

Terry L. Grover

Health/OMAP, (503) 945-6536

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



“SPAM” continued...

It can create productivity costs and threaten IT systems and network integrity. In addition, it is increasing the task faced by regulatory authorities because of its content.

No ‘Spoofing’

Spoofing is the forgery of an email header so that the message appears to have originated from an entity or location other than the actual source.

Spammers may use spoofing to route spam through a reputable organization in an attempt to lure recipients to open and respond to their messages.

What problems are caused by spam?

- Negative effect on users’ confidence in using email.
- A spam explosion could mean the end of email as an effective form of communication.
- Privacy becomes an issue as email addresses and personal information are collected.
- Illegal/offensive content, misleading and deceptive trade practices and burdensome financial and resource costs.
- Misuse/abuse of computing resources - Spam containing no illegal or inappropriate content can still cause damage due to the massive amounts of messages and consumption of bandwidth and computing resources.

DHS spam key facts:

In work email accounts, the volume of Spam and the time spent reading and deleting the Spam appears to be relatively small. However, that relative “success” against Spam comes at a price. The costs and consequences of Spam in the work email accounts are often hidden from the average worker. Email users feel overwhelmed by Spam, but in fact what they see is only the tip of the iceberg.

- The state email servers filter out approximately 85% of the Spam that is sent to DHS.
- The remaining 15% that DHS still receives is still an extraordinary amount of Spam.
- For example, only 61% of the email received by DHS from April 15 – May 1st could be classified as legitimate. The rest was spam.

What is DHS doing to address spam?

DHS is doing two things:

- 1) Educating employees
- 2) Working on implementing a “Secure Messenger” system that has been purchased. The “filters” have been tested and which significantly reduced the amount of SPAM received by DHS staff.

So, what should I do when I receive spam that gets through the filters?

Unfortunately, there is no “silver bullet.” Some spam still finds its way to your email box because spammers are sneaky. The best ways to deal with the spam that does make it through the filter is to just delete it.

Building Entry Badges

Are we protecting our photo ID?

Badges allowing access to a building should be safely stored. Many times employees hang their photo ID around their mirrors at work. Some leave it hanging in cars in parking lots or at home. This can attract thieves, as it gives them access to the buildings and a lot more than just the contents of a car.

So next time you store your photo ID...Just think about its access potential!

Awareness and Education Program Update

ISO launches revised electronic versions of mandatory training modules

WHAT: *Privacy Security, DHS and You!* goes electronic! In addition, the session is now in two parts. Module (1), will give all employees the skills and knowledge needed to identify and counter some fundamental security and privacy risks and requirements. Module (2) is designated for employees who work in areas where there is direct client contact or in situations where handling confidential client information is routine and addresses the requirements around the HIPAA Federal Privacy Rule.

Currently, DHS staff are required to enroll for the Privacy/Security DHS & YOU Netlink within 30 days of hire—this will still apply, however, the Netlink session will now be replaced with enhanced versions that new employees can access right from their desks.

WHO: New DHS employee volunteers and those affiliated by contract service are required to complete module 1 within 30 days of hire.

New DHS employee volunteers and those affiliated by contract services who work in areas where clients are served or in situations where handling confidential client information is routine must complete both module 1 and module 2 within 30 days of hire.

*Hospitals, training centers and group homes will be able to maintain the current practice of acquiring the content from ISO for classroom delivery for both modules.

WHEN: July 2, 2007

WHY: DHS employees using and managing information must be aware of their roles and responsibilities in order to protect the confidentiality, integrity, and availability of this information. They should understand the policy, procedure and practices, as they are responsible for providing security of this information. Accountability and expectation can be fully derived only from an informed, well-trained and aware workforce.

WHERE: To access this new CBT, go to the online DHS Learning Center: <https://dhslearn.hr.state.or.us>

Registration Instructions:

1. Go to “Courses and Registration” in the left-hand purple-shaded area.
2. Click on the icon that says “Find a course and register.”
3. Type “ISO” in the keyword box and click on “search.”
4. Selection of courses shows up in lower left-hand box.
5. Click on the link to get to a page that launches the courses.

The information provided in the Privacy/Security Update is intended for employees of the Oregon Department of Human Services. It is not intended as advice, legal or otherwise, to any entity outside of the department.

DHS BCP program coordinators

Program sponsor: *Clyde Saiki*, DHS deputy director, 503-945-5731

Program manager: *Patty McCary*, ISO, 503-945-6996

Manager: *Kelli Heflin*, ISO, 503-947-5230

Administrative Services

Linda Riddell, Facilities, 503-945-5817

Sharon Domaschofsky, Facilities, 503-947-5018

Dennis Wells, OIS, 503-945-6573

Dave Wallace, OIS, 503-945-5992

Jeremy Emerson, OC&P, 503-945-6878

Kelly Stoll, OC&P, 503-945-5696

Julie Davie, HR, 503-945-6380

Gary Whitehouse, OPA, 503-945-6934

Debby Williams, OPAR, 503-378-5620

Jan Lemen, FDM, 503-378-3477

Children, Adults and Families

Leona Gildersleeve, CAF, Field Admin, 503-945-7000

Irvin Minten, CAF, 503-373-1200 (ext. 543)

Health Services

Maynard Hammer, OSH, 503-945-2866

Dusty Charters, OSH, 503-947-1080

Steve Modesitt, HS/PH, 971-673-1293

Dale Elder, HS/DMAP, 503-945-6589

Robert Furlow, EOTC, 541-276-0810 (ext. 331)

Nick Reed, EOTC, 541-276-0991 (ext. 431)

Edie Woods, HS/OMHAS, 503-945-6189

Seniors and People with Dis.

Bob Clabby, SPD, 541 276-4511 (ext. 470)

Donna Weaver, SPD, Field Services Manager, 503-945-5977

Conrad Bozlee, SOCP