Security :: Security Resources for ITS Support Staff

IT personnel are expected to have a solid understanding of information security issues, both in general and how they apply specifically to the use of computers on the HSU campus. For ease of use, this page brings together a number of security-related resources - you're encouraged to review and become familiar with them.

What to do in case of a security incident

IT support staff involved with investigating computers that may have been compromised by a security incident should thoroughly review the HSU Compromised Host IT Staff Procedure [1]. If a computer security emergency occurs, everyone needs to know what their responsibility is immediately; this is one event that's not an "on-the-job" learning opportunity - you need to be prepared.

Securing protected information

HSU mandates encryption [2] of all protected information stored on University-owned devices. Encryption is one of those areas where things can go irretrievably wrong very quickly, so IT staff need to be up to speed on the encryption methods and programs supported by HSU. Please take some time to review the section of this website that deals with encrypting protected information [3].

Security-related forms

Because of the sensitivity and legal requirements surrounding confidential data and other information processing and storage activities, security-related activities involve many forms. For your convenience, we've assembled links to all relevant forms [4] on one page.

SSL certificates

CSU has partnered with InCommon [5] to provide a secure certificate service through Comodo Certificate Services. This service allows an unlimited number of SSL Server Certificates to be issued for Humboldt State University. Certificates may be requested for up to three years. To request a certificate, contact the Information Security Office at (707) 826-6125 for an access code and submit server signing certificates [6]. Check out the SSL Server Certificate FAQ [7] for more information.

What you need to know about HSU networks

All of the networking elements described below have an impact on the security of HSU's computer networks as a whole, so please review this information carefully. As always, if you have questions about security issues, please refer them to iso@humboldt.edu [8].

Printer/Copier Virtual LAN (VLAN)

Digital printers and other multi-function devices [9] store images of every document that passes through them, which makes them a primary target for compromise by hackers. For this reason, protected VLANs have been established to protect information flowing through printers and copiers; when submitting Dynamic Host Configuration Protocol **(**DHCP) registration forms, it's important to indicate when a multi-function device is involved.

Administrative Building Virtual LANs (VLANs)

Each permanent building on campus has at least one administrative VLAN which links departmental computers that may process or store protected information.

Academic Building Virtual LANs (VLANs)

Each permanent building on campus has at least one academic VLAN for uses such as computer labs. Computers that have access to or contain confidential protected data should not be placed in the academic VLAN.

Affiliations and Groups

The terms Affiliations and Groups are used to describe the roles and relationships people have with the University. Affiliations are represented in two ways: in the user’s record and as a member of a particular group. At HSU, affiliations are published in LDAP user records in the eduPersonAffiliation attribute, and in AD and LDAP under HSU-Groups. Read more [10].

Internet-Facing Devices

To register a system that needs to be available over the Internet, log into the Internet Facing Device registration system [11]. If you need assistance accessing this site, call TNS at (707) 826-5000 or email netops@humboldt.edu [12].

Port Security

If more than three computers are attached to a single jack or port, the port will disable itself. Contact TNS at (707) 826-5000 or email netops@humboldt.edu [12] if additional jacks are required. Follow these procedures [13] to block outbound ports and address ranges.

Vulnerability Scans

TNS routinely conducts confidential scans of HSU networks to identify systems with weak network security. Departments are notified if any of their systems are found to have vulnerabilities and requested to remediate those systems.

Dynamic Host Configuration Protocol (DHCP)

Computers connected to the HSU network are required to use DHCP so that they function correctly.

Related Topics

Tools & Resources [14], Data Protection [15], Security [16]

Source URL: http://www2.humboldt.edu/its/security-itsupportinformation

Links:
[1] http://www2.humboldt.edu/its/security-compromisedhostprocedure
[2] http://www2.humboldt.edu/its/glossary/5#term239
[3] http://www2.humboldt.edu/its/security-encryption

[4] http://www.humboldt.edu/its/security-forms
[5] http://www.incommonfederation.org/index.cfm
[6] https://cert-manager.com/customer/InCommon/ssl?action=enroll
[7] http://www2.humboldt.edu/its/ssl-certificate-faqs
[8] mailto:iso@humboldt.edu
[9] https://www.humboldt.edu/its/security-multifunction
[10] http://www2.humboldt.edu/its/sites/its/files/docs/HSU-Affiliations-1-11.docx
[11] http://tns.humboldt.edu/ifd
[12] mailto:netops@humboldt.edu
[13] http://www.humboldt.edu/its/sites/its/files/docs/its-practice-outbound-ports.pdf
[14] http://www2.humboldt.edu/its/category/quicklinks/tools-resources
[15] http://www2.humboldt.edu/its/category/quicklinks/data-protection
[16] http://www2.humboldt.edu/its/category/quicklinks/security