Security :: Tools and Resources

Tools

HSU's information security infrastructure comprises the tools and equipment the campus employs to protect University-owned computers and networks. This infrastructure is designed to be as unobtrusive as possible while still maintaining a high degree of protection against malware [1], hackers, and data breaches:

- Campus border firewall [2]. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware, software, or a combination of both.
- Encryption [3]. Encryption converts data into a secure form that can be safely moved around and helps HSU meet its obligations under various data protection laws and policies. One of the most effective ways to protect personally identifiable or other confidential information stored on a computer is to encrypt it.
- Network Access Control [4] (NAC). Designed to proactively prevent malware or hackers from gaining access to the network. At HSU, this is tackled at two levels: the network perimeter [5], where the HSU networks meet the Internet, and the individual system level [6].
- Password management [7]. Every student, staff, and faculty member is provided with a unique HSU User Name when they officially enter the university population. Each individual must also create (and periodically change) their own secure password, which is used in combination with their User Name to permit access to the relevant systems based on their university role.
- Protected Information Discovery Tools [8]. Personally Identifiable Information (PII [9]) is an umbrella term for information linked to an individual's identity, such as Social Security Numbers, drivers' license data, and credit card or bank account information and which can be used to facilitate identity theft. PII Discovery Software is used to scan University-owned computers to assist in identifying such data so the appropriate action can be taken to secure it.
- Secure wireless [10]**.** The secure wireless network at HSU provides all the benefits of the regular wireless service - anytime, anywhere access to the Internet. By using secure wireless, staff, faculty, and graduate students can access more of the wired network, including departmental file shares and wired printers, enabling them to work productively anywhere on campus using personal or University-owned devices.
- Virtual Private Network [11] (VPN). A secure communication channel that enables staff and faculty to access their office computers from off campus via a secure web interface.
- Virus protection tools [12]. Sophos Anti-Virus is installed on all HSU-owned computers, and may be installed free of charge on personally-owned computers by students, staff, and faculty.
- Vulnerability Scanning [13]. Vulnerability scans provide critical information to the Information Security Office and management as part of the risk assessment process for campus systems.

Resources

- Third Party - Contract Language, Guidelines, Policies & More [14]. CSU policies provides for direction and support for managing third party relationship and for granting access to various HSU resources and third party contract language.
- Mobile Device Security [15]. Do's and don'ts to keep your mobile devices and the data stored on them secure against hacking and other security issues.
- Online Cloud Storage and Email [16].Frequently Asked Questions and Answers relating to storing data in the cloud shares and sending email and attachments securely.
- Forms [17]. For convenience, all HSU security-related forms are linked from a single web page.
- Information Security Training [18]. HSU provides Information Security Awareness online and

on-campus training materials designed to provide staff and faculty with the knowledge they need to secure information resources.

- Secure Disposal of Paper / Shredding and Electronic Media [19]. Any data storage medium - paper, computer, scanner, copier, hard drive, tablet, smartphone - should be treated as if it contained protected data and must be securely wiped prior to transfer or disposal.

Guidelines and Procedures

- Compromised Computers and Incident Reporting Procedures for Students and Employees [20]. There are many security threats of which to be aware and protect against in order to ensure sensitive information remains secure. These threats are not just caused by sophisticated hackers; they're also caused by a lack of attention or care by people entrusted with sensitive information. **Potentially-compromised system incidents must always be referred to the Campus Information Security Officer at (707) 826-3815 or the University Police Department at (707) 826-5555.**

- Compromised Host Response IT Staff Procedure [21]. Procedures for a networked computer that is suspected of being compromised by a virus or other malware attack.
- Multifunction Copier Devices [22]. Site preparation, network security settings, scan to folder
- Secure Media Transfer and Disposal Procedures [23]. Procedures to prevent the inadvertent release of confidential, protected, or personally-identifiable information contained on electronic storage devices when physical possession or stewardship changes.

Security for IT Support Staff

For ease of use, this page [24] brings together a number of security-related resources.

Related Topics

Tools & Resources [25], Security [26]

Source URL: https://www.humboldt.edu/its/security-tools-and-resources

Links:
[1] https://www.humboldt.edu/its/glossary/5#term200
[2] https://www.humboldt.edu/its/security-firewall
[3] https://www.humboldt.edu/its/security-encryption
[4] https://www.humboldt.edu/its/security-networksecurity
[5] https://www.humboldt.edu/its/security-networksecurity#Perimeter_protection
[6] https://www.humboldt.edu/its/security-networksecurity#system_protection
[7] https://www.humboldt.edu/its/security-passwordsecurity
[8] https://www.humboldt.edu/its/security-protectedinformationsurvey#tools
[9] https://www.humboldt.edu/its/glossary/5#term225
[10] https://www.humboldt.edu/its/secure-wireless
[11] https://www.humboldt.edu/its/services/virtual-private-networks-vpns
[12] https://www.humboldt.edu/its/security-virusprotection
[13] https://www.humboldt.edu/its/node/2597
[14] https://www.humboldt.edu/its/security-third-party
[15] https://www.humboldt.edu/its/mobile-device-security
[16] https://www.humboldt.edu/its/cloud-storage
[17] https://www.humboldt.edu/its/security-forms
[18] https://www.humboldt.edu/its/node/2586
[19] https://www.humboldt.edu/its/security-securedestruction

[20] https://www.humboldt.edu/its/security-incidentresponse
[21] https://www.humboldt.edu/its/security-compromisedhostprocedure
[22] https://www.humboldt.edu/its/security-multifunction
[23] https://www3.humboldt.edu/iso/ITC016-media-destruc-proc-appr-rev 9-19-12.pdf
[24] https://www.humboldt.edu/its/security-itsupportinformation
[25] https://www.humboldt.edu/its/category/quicklinks/tools-resources
[26] https://www.humboldt.edu/its/category/quicklinks/security