PM 2023–02 [Supersedes PM 2009-12]
Thomas A. Parham, Ph.D.
March 8, 2023

USER RESPONSIBLE USE POLICY

POLICY

Consistent with published CSUDH Information Security and Privacy Policy, this policy outlines the roles and responsibilities of the Users. This policy is further supported by related IT standards and guidelines that facilitate University compliance with the recommendations, audit requirements, actions, and safeguards necessary to mitigate risks, protect information assets, and user data.

PURPOSE

California State University, Dominguez Hills (CSUDH) provides many technology tools to its students, faculty, employees, guests, visiting scholars, interns, and vendors (Users) in support of the university's teaching and research mission. These tools include computers, software, communication tools (email, chat), access to internal networks (intranet), access to external networks (internet), as well as telephone systems, voice mail, fax, photocopiers. These resources are provided to encourage academic inquiry and the sharing of information, while seeking to protect the right to privacy, freedom of expression, freedom from intimidation and harassment, rights to intellectual property, and security of information. Maintaining such an atmosphere requires that all members of the university community use these resources responsibly and with respect to the rights of others. CSUDH requires that these public resources be used in a responsible way, ethically, and in compliance with all legislation and other CSUDH, CSU, State, and federal policies and laws. Technology communications is a rapidly changing area; this policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing the system of their obligation to use common sense and good judgment and check with I.T.

SCOPE

All Users of CSUDH technology, including full-time, part-time, and temporary students, faculty, employees, guests, visiting scholars, interns, and vendors, must follow the requirements of this policy. The requirements defined in this policy are applicable to all data systems, and services owned and/or managed by CSUDH and/or CSU. It governs your use of all computer hardware, software, infrastructure, cloud, and services owned, licensed, or managed by the CSUDH and/or CSU. In order to access these resources, you must agree to comply with this policy as well as all applicable CSUDH and/or CSU policies and regulations, and local, state, and federal laws.

GENERAL POLICY AREAS

A. Acceptable Use of Assets

Assets include, but are not limited to, physical equipment, such as desktop computers, servers, printers, laptops, telephones, mobile devices, and removable media (such as USB flash drives), as well as systems, cloud, and services, such as the organizational network, internet, voicemail, and more (Any new system that may rollout at the future would also fall under this policy). University data is also considered to be an asset. All University assets must be used in accordance with policies, standards, and guidelines of CSU and CSUDH and the policy set forth below.

1. CSUDH (CSU Incidental Use) allows limited use of the network, systems, and devices for personal reasons (personal correspondences, online banking, etc.), but personal use must not be abused. Personal use must:
    a) Not have a negative impact on overall employee productivity.
    b) Not cause additional expense to the university.
    c) Not compromise university security and compliance in any way.
    d) Not disrupt network performance.
    e) Not violate any other Federal, State, CSU or CSUDH policy.
2. CSUDH assets and systems may not be used for illegal or unlawful purposes, including copyright infringement, obscenity, personal gain, libel, slander, fraud, defamation, plagiarism, unlawful threats, harassment (harassment as defined per the CSU Discrimination, Harassment and Retaliation policy) forgery, impersonation, illegal gambling, soliciting for pyramid schemes, and computer tampering (e.g. spreading computer viruses).
3. I.T. shall approve access and/or purchase technology, devices, applications, or services at CSUDH.
4. I.T. assets, such as laptops and mobile devices, are intended to be used only by the people to whom they have been issued.
5. Users will endeavor to protect all University-managed I.T. assets at all times. Recommended efforts to keep assets secured and under the control of the user include, but are not limited to:
    a) Locking down laptops with a locking cable or storing them in a locked drawer or cabinet when leaving them in the office.
    b) Ensuring the workstation is locked (screen/keyboard) whenever walking away from it.
6. Access to CSUDH systems and devices is controlled through individual accounts and passwords, as outlined in the Password and MFA Standards and in the CSU Access Control Policy.
7. All voicemail boxes will be protected with a PIN (personal identification number). Easy-to-guess or previously used PINs will be blocked by the system. PINs must not be shared with others.

8. Removable media, such as USB flash drives, CDs, etc., may be used with the following requirements:
    a) Information should only be stored on removable media when required in the performance of the user’s role (e.g. USB shared between two employees during a conference).
    b) The use of removable media to introduce unauthorized software into the CSUDH environment is strictly prohibited, including malware.
    c) Mobile devices (e.g. smartphones, tablets) are not permitted to be used as removable media to transfer or store any CSUDH or student data.
    d) Any unknown removable media that is found unattended must be reported to the I.T. Department and NOT inserted into any CSUDH issued device.
    e) End users are encouraged to take reasonable measures to secure removable media (e.g. storing it in a secure/locked location when not in use; not sharing with unauthorized users).
    f) Use of CSUDH removable media is not allowed on external or non-University-issued systems.
    g) Upon completion of the assigned duties, all data shall be deleted from the removable media, in accordance with NIST SP 800-88 Rev. 1.
    h) All removable media must be turned in to Service Management for proper disposal when no longer required for business use, in accordance with NIST SP 800-88 Rev. 1.

B. <u>Electronic Communication and Internet Use</u>

The use of CSUDH communication and internet systems and services (including email, list servs, instant messaging, voicemail, forums, social media, and more) is provided in order to perform regular job duties. CSUDH Communication systems must be used with respect, common sense, and in accordance with the following requirements:

1. The email systems, distribution lists, and other messaging services used at CSUDH are owned by the university and are therefore its intellectual property (IP). This gives CSUDH the right to monitor and record any and all email traffic passing through its email system. This monitoring may include, but is not limited to, incidental reading by I.T. staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency. These individuals shall maintain the confidentiality and privacy of the information unless otherwise required to disclose by law or policy of CSU or CSUDH.
2. In addition to the Toro Alert system for emergency communications by University Police, CSUDH often delivers official communications via email. As a result, Users of CSUDH with email accounts are highly encouraged to check their email in a consistent and timely manner so that they are aware of important university announcements and updates, as well as for fulfilling business and role-oriented tasks.

3. Electronic communication, list servs, and internet must not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, cryptocurrency mining, obscenity, libel, slander, fraud, defamation, plagiarism, harassment (as defined by the CSU Discrimination, Harassment and Retaliation policy), discrimination (as defined by the CSU Discrimination, Harassment and Retaliation policy), intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses and malware).
4. CSUDH communication platforms, distribution lists, and internet are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared storage such as Dropbox). Individual use of resources will not interfere with others' use of CSUDH email system and services.
5. Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.
    a) Users are not to give the impression that they are representing or providing opinions on behalf of CSUDH unless otherwise authorized.
6. CSUDH prohibits use of email or other messaging platforms for mass unsolicited mailings, advertisement, chain letters, and competitive commercial activity unless preapproved by CSUDH. List servs created for Union chapters are to be used for union communications. Many of the CSU bargaining unit contracts provide for access to the campus e-mail system for official union communications. Nothing in this section will limit or abridge these rights.
7. Any allegations of misuse should be promptly reported to Information Security Office. If you receive an offensive or suspicious email, do not forward, delete, or reply to the message. Instead, report it directly to the Information Security Office.
8. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list and is responsible for doing so in the event that their current email address changes.
9. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with Systemwide Records Information Retention and Disposition Schedules.
10. Email access will be terminated by the University when the employee, student or other third party terminates their association with CSUDH, unless the University has approved an alternative arrangement. CSUDH is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment, the academic studies or other active affiliation with the University has ceased. University administration has the right to terminate any prior arrangements.
11. Users shall not send sensitive information that is not appropriately protected (encrypted). (Appropriate means of protection include but are not limited to Dropbox Secure Folders)
    a) Users shall take extra precautions when transmitting University and/or other regulated information via electronic communications. (For example: Confidential Research information or Sensitive student information, credit card information.) Sensitive material should be marked and encrypted appropriately. Keep in mind

that all email messages sent outside of CSUDH become the property of the receiver.

12. Users are not permitted to automatically forward emails received by their CSUDH account to an external email address or other messaging system.
13. Consistent with the CSU Information Security Responsible Use Policy, CSUDH assumes no liability for direct and/or indirect damages arising from the user's use of CSUDH's email system and services. Users are solely responsible for the content they disseminate. CSUDH is not responsible for any third-party claim, demand, or damage arising out of use CSUDH's email systems or services.
    a) However, email users are expected to remember that email sent from the University's email accounts reflects on the university. Users should strive to conduct themselves with normal standards of professional and personal courtesy and conduct.
14. In the normal course of system and information security maintenance, both preventive and troubleshooting, system administratorsand service providers may be required to vie w files and monitor content on the CSU and campus networks, equipment, or computin gresources. These individuals shall maintain the confidentiality and privacy of informatio n unless otherwise required by law or CSU/campus policy.
15. Users are permitted to remotely access the University network while offsite. Users must use the approved VPN service(s). Users will be required to authenticate using multifactor authentication (MFA). Only authorized users are permitted to access the network through VPN.

C. Data Security and Privacy

Maintaining the confidentiality, integrity, and availability of the university data is paramount to the security and success of the university. The following requirements are defined to keep data secure and handled appropriately.

1. All university data is owned by CSUDH and, as such, all users are responsible for appropriately respecting and protecting all data assets.
2. Users must keep all data secure by taking sensible precautions and following requirements defined in this policy, CSU Data Classification Standards, and the data-handling requirements defined in the CSU Data Classification standard. This standard outlines the requirements for creating, using, storing, transmitting, archiving, and destroying data. The Information Security Office is able to provide assistance on classifying and giving guidance.
3. Data must be classified based on sensitivity, as defined in the CSU Data Classification Policy. Data must be classified as Level 1, Level 2, and Level 3 Data at each classification level must be safeguarded and handled appropriately in accordance with the CSU Data Classification Policy.
4. Users may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to CSUDH or another individual without authorized permission.

5. Users will only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.
6. Extraction, manipulation, and reporting of CSUDH data must be done for approved educational purposes only.
    a) Personal use of organizational data, including derived data, in any format and at any location, is prohibited.
7. Users will follow all university-sanctioned data removal procedures to permanently erase data from devices once its use is no longer required, as defined in the CSU Data Classification Policy. Data must be retained for the length of time defined in the Systemwide Records Information Retention and Disposition Schedules.

D. Incident Response and Reporting

CSUDH has an incident response program for efficient remediation of the security incidents. Users are expected to comply with the following requirements in order to ensure effective and efficient incident remediation:

1. Users must report any suspected security incident to the Information Security Office, including but not limited to lost/stolen equipment, suspected malware infection, compromised credentials, and any other possible compromises of CSUDH systems and/or data.
2. Users must cooperate with incident response processes, such as forfeiting their equipment to Service Management for investigation if it is potentially compromised.

OWNERSHIP AND PRIVACY ISSUES

The CSUDH has broad responsibilities with respect to protecting its information assets. These include but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information. CSU policies related to these activities are available in the CSU Policy Library.

The CSUDH retains ownership or stewardship of information assets owned (or managed) by or entrusted to the CSUDH. The CSUDH reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include but is not limited to monitoring communications across network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational.

The systems are the university’s property as well as, for access and security purposes, the data they contain. We respect our Users’ right to privacy; however, we grant access to our systems for business use. Employees and students must not expect that information contained in these systems is private. The university reserves the right, from time to time, for commercial, legal, or otherwise valid reasons, to read, monitor, control, and access user files and messages created, saved, transmitted, or received. In the event of intercepted illegal activity, we will bring them to the attention of the appropriate authority without prior notification to the sender or receiver.

NONCOMPLIANCE

Users who violate any of the above policy may be subject to corrective action, including disciplinary action where appropriate. Individuals who violate the law, including U.S. copyright law and software licensing agreements also may be subject to criminal or civil action by the copyright or license owners.

Violators are subject to any and /or all of the following:

- Loss of computing and networking access
- University disciplinary actions
- Civil proceedings
- Criminal prosecution

Any discipline will be administered pursuant to the applicable provisions of the affected employee's collective bargaining agreement and/or the applicable campus policy.

REFRENCE

- Data Classification Policy
- Information Security and Privacy policy
- Access Control Policy
- Retention Policy
- Mobile Device Policy
- [Others…]

Approved: Thomas Parham Date: 3/8/2023

Thomas A. Parham, Ph.D.
President

Policy Title	User Responsible Use Policy
Policy Category	Information Technology
Policy Owner	Sara Hariri
Policy Approver(s)	Dr. Thomas Parham
Related Policies	Information Security and Privacy policy, CSU Responsible Use policy
Related Procedures	
Effective Date	Date of Signature
Next Review Date	

Revision History

Version	**Change**	**Author**	**Date of Change**
1.0	N/A	Group	N/A