User Standards in Support of Responsible Use of Information Technology Resources

Policies

Responsible Use of Information Technology Resources Policy

User Standards in Support of Responsible Use of Information Technology Resources

Policy on Data and Data Access

Information Security Program Administration Policy

(D102) Network Security

(D103) Server Security

(D104) Workstation Security

(D105) Credential Security

(D106) Email

(D110) Operational Management Policy

(D111) Stony Brook University Google Apps for Education Acceptable

These user standards expand upon University Policy: "Responsible Use of Information Technology Resources" and are incorporated by reference. They outline the responsibilities each member of the community accepts when using the University's information technology (IT) resources. It constitutes a minimum set of standards for all areas of the University. Units may issue additional unit-specific guidelines, but additional guidelines must be consistent with this document and cannot supersede it or its standards.

#1: Be considerate

IT resources are provided by the University to help students, faculty, and staff succeed in activities consistent with the University's mission and priorities.

Do:

- Respect the rights of other users to carry out their activities
- Respect that the University's IT resources have a finite capacity

Don't (examples):

- Attempt to deliberately degrade performance or deny service
- Consume an unreasonable amount of resources or interfere with the authorized activity of others
- Propagate email spam, computer viruses, or malware
- Engage in "spamming" (spreading email or postings widely and without good purpose)
- Communicate with an individual who has specifically requested not to receive communications from you

#2: Protect yourself and others

Take appropriate information security precautions to reduce risk, to protect the privacy of you and others, and to help protect the University's resources and data.

Do:

- Keep your credential(s) (e.g., NetID) private.

Use and Data Security Policy

(D112) Electronic Mail (Email) Retention Policy

(D120) Web Resources

(D121) Internet Videoconferencing and Virtual Meeting Rooms

(D123) Domain Name Policy

Plan to Combat Unlawful Distribution of Copyrighted Material

Faculty/Staff Personal Computer Policy

Acknowledgement and Compliance Statement

Brightspace Use Policy

- Be forthright and transparent in personal and device identification.
- Use a fully supported version of antivirus or endpoint security software (e.g. Symantec EndPoint Protection) on devices you own or manage. Configure it to automatically apply updates and periodically assure that definitions are up to date.
- Enable firewall protection on devices you own or manage.
- Take steps to ensure that security patches to your computer's operating system and any installed applications are installed in a timely manner.
- Back up critical data on a regular basis.
- Exercise care in opening emails, and email attachments, and links to websites.
- Be aware of malicious web sites, and clicking on links to unknown websites.
- Install only properly licensed versions of software, and keep them updated.
- Take care to only connect only to trusted wifi wireless hotspots.

Don't (examples):

- Share or give your credentials away.
- Transfer or share your access privileges without proper authorization.
- Use former privileges after graduation, transfer, or termination, except as explicitly authorized by the University.
- Attempt to hide your identity while using University IT resources, except when anonymous access is explicitly allowed.

#3: Follow applicable laws, policies, and rules:

Applicable laws, policies, rules, and codes of responsibility apply to the IT environment just as they apply in all other University contexts.

Do:

- Become familiar and comply with applicable University policies when using IT resources, such as those on: Academic Integrity, Copyright, University Student Code of Responsibility, Sexual Misconduct, Human Resources, Research Misconduct, Information and Data Governance, Finance, and Facilities.
- Comply with applicable local, state, and federal laws and regulations.
- Comply with applicable licenses and contractual commitments of the University.

- Respect the rights of copyright owners in the use, distribution, or reproduction of copyrighted materials.
- Adhere to the terms of service for all offered IT services.

Don't (examples):

- Upload, download, distribute, or possess illegal material.
- Use University IT resources for private commercial purposes, or for personal financial or other gain.
- Send forged email.
- Misuse resources to allow users to hide their identities, or to interfere with other systems or users.
- Send terrorist threats or "hoax messages".
- Use privileged access for other than authorized activities.
- Use University resources for partisan political activities.
- View, copy, or distribute the personal electronic files of another individual without permission.
- Download, distribute, or share copyrighted material without the express permission of the owner.
- Make more copies of licensed software than the license allows.
- Use the software for purposes not allowed for in the license.
- Operate a peer-to-peer file sharing service that disseminates copyrighted material.
- Facilitate access to campus Intellectual Property by those whose use is not authorized.

#4: Maintain the Operational Integrity and Security of University IT Resources

In order to ensure that IT resources are available for use by authorized users, the integrity and security of IT resources must be maintained. The University reserves the right to remove content, disable web sites, disable accounts, deactivate IDs, and block devices using the University network in order to protect the integrity and security of University IT resources.

Do:

- Alert campus authorities when you learn of compromised account credentials (e.g., NetID, password).

- Alert campus authorities if you find that you have access to data or systems that, which, are not consistent with your role, responsibilities, or authority.
- Understand that the University monitors electronic communications and activity in the course of protecting University assets. Investigations of unauthorized use, illegal activity, misuse, or systemic problems may require observation by authorized University personnel or their agents.

Don't, unless authorized by the University (examples):

- Attempt to circumvent security mechanisms.
- Access or attempt to access or use data maintained by other users or by the University that you are not legitimately authorized to access.
- Look for or purposely exploit security flaws on systems or networks that do not belong to you.
- Release computer viruses or worms.
- Corrupt or misuse data.
- Alter or destroy data without authorization.
- Use unauthorized network addresses.
- Circumvent systems that enforce access, management, or quotas.
- Provide or support a public-facing service, such as a web site or application, that is unrelated to University authorized activities.
- Install or connect devices to the University network that could potentially degrade or deny services, including, but not limited to routers (wifi and wired), wifi access points, switches, proxy servers, gateways, compromised / infected personal devices and Dynamic Host Configuration Protocol (DHCP) appliances.
- Remove or modify University IT systems or devices without approval.

#5: Cooperate with University IT Professionals

From time to time your activities may interfere with operation of IT resources, even though they may not clearly be prohibited by the Responsible Use of Information Technology Resources Policy. In such cases, a University IT professional may contact you and require you to discontinue an activity. You are expected to comply with such instructions. Once you have received such a warning, continued activity of the same kind will be treated as a violation of the Responsible Use of Information Technology Resources policy.