Title: Social Media Usage Policy Policy: 6810

Purpose

Social Media and Web Site technologies present new security challenges to the Information Technology network infrastructure as well as a threat to Personally Identifiable Information ("PII") of individuals within the Virginia State University community. The instant VSU Social Media Usage Policy shall be compliant with the Commonwealth's Information Technology ("IT") Security Standards as well as best practices for internet and network security to help mitigate any threats that may result from social media usage. This instant policy also strives to bolster the position of the Anti-Harassment and the Anti--Discrimination policies of the University.

Guiding Principles

The guiding principles for this policy is to establish safe, practical and responsible employee (intern, contractor, full-time and/or part-time employee) usage rules and guidance for the engagement of social media access for the protection and security of all employees and the University. The instant policy is also to address the responsibilities of official and non-official usage of social media on behalf of VSU employees, interns, contractors and the like.

Scope of Policy

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators, and student interns) who access and/or utilize the information technology infrastructure of VSU.

Responsibility and Duties

A. All Users/Employees

a. Employees must be aware and educated on the Acceptable Use Policy of the University as well as the other IT Policies, Human Resources and Anti-Discrimination policies of the University and conduct themselves in compliance with same.
b. Employees must be aware of the effect of any of their actions on the internet when using Social media and the impact on their reputation and that of the University.
c. Employees should not indicate on their **personal** social media accounts that they are representing the views and opinions of the University.
d. Employees should use their best judgment when engaging on social media sites, which includes not posting material that is inappropriate, harassing or harmful to fellow employees
or clients/students of the University. The employee shall not engage in cyberbullying.
e. Employees shall not publish, post or disseminate any commentary, images or content that are defamatory, pornographic, libelous, harassing or create any hostile work environment through any social media medium.
f. Employees shall not publish, post, release or otherwise disseminate any information that is considered University confidential, proprietary, trade secret and/or not public.
g. Employees must contact University legal counsel if any behavior or information disseminated within social media garners any media, human resources or legal attention.

h. Employees must disengage from any dialogue in social media if any case wherein the encounter becomes antagonistic or threatens the life, safety and well-being of others. The employee should report this encounter to their immediate supervisor.

1. Employees shall get permission from other employees, clients and/or students prior to posting photos or references on social media of that other person.

J. **Personal** social media usage must not interfere with the employee's employment responsibilities at the University. Employees are reminded that there is no expectation of privacy granted to them on the assets and network belonging and/or leased to the University.

k. If Employees post information to their **personal** social media accounts involving the University, said employee must publish a disclaimer that the "Personal opinions on the site are my own and do not represent any official Virginia State University positions, strategies or opinions."

l. Any online activity that violates the policies of the University or any state or federal law may subject the employee to disciplinary action and/or termination in addition to and separate from any law enforcement action.

m. All employees shall report to their supervisor any questionable or other postings in **personal** social media that may constitute a breach of this instant policy or any other University policy.

n. Employees should be mindful of copyright and intellectual property rights and protections for anything they utilize and/or post on social media.

B. Supervisors, Management, Human Resources

In addition to all of the requirements for general users, this designated group of users have the following additional responsibilities:

a. All reports made from employees shall be memorialized in writing after receiving the initial complaint and, if possible, meeting with the reporting employee.

b. All reports shall be elevated to the appropriate parties for further review, whether it is University Counsel, Human Resources Manager, Campus Police and the like.

c. All reports shall be kept confidential, except for when being elevated to the appropriate parties for further action.

d. No retaliation shall come to the reporting employee from any employee in the reporting chain or from the employee that the report concerns.

e. Thoroughly cooperate and facilitate with any investigation, regardless if it is University internal or external law enforcement.

C. VSU Public Information Office and/or Media Relations Agent and Faculty

a. Employees of the Public Information Office and/or Media Relations are permitted to post approved, non-confidential University content to the University public social media websites and outlets. This permission does not grant the right or permissible use of any of the University content on any personal social media site.

b. Employees in this role may only post from University approved accounts that represents the official University position.

c. Employees of said office do not need permission from the Chief Information Security Officer to post the content, said permission should come from their immediate supervisor.

d. Employees, under no circumstances, are permitted to violate any federal or state law in the disclosure of information (such as HIPAA, FERPA, etc.).
e. Faculty may publish non-confidential, academic information on class websites and social media sites that facilitate learning of the students.
f. Employees may not improperly use or post materials protected by copyright, trademark, patent, trade secret, data rights or other intellectual property.
g. Employees must conduct themselves in a professional and honest manner in all public communications on behalf of the University.
h. Employees must monitor the official social media sites that he/she posts to on a regular basis to ensure accuracy and integrity of the information.

Definitions

The IT security definitions and terms can be found in the COY ITRM IT Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.viminia.gov/library.

Employees, used in conjunction with "user" refers to Contractors, Interns, Faculty, Staff and Administration, Full and/or Part-time employees who use the Information Technology resources of the University.

Social Media includes the usage, but is not limited to: blogs, wikis, microblogs, online journals or diaries, personal web sites, message boards, chat rooms and services, electronic newsletters, online forums, social networking sites and other sites that allow and enable users to share information with others in a contemporaneous manner.

Exceptions to this Policy

If the user determines that compliance with the provisions of this policy or any related information security policy would adversely impact a business process of the agency, the user may request approval to deviate from a specific requirement by submitting an exception request to the VSU Information Security Officer (ISO). For each exception, the requesting the user shall fully document:

1. The business need,
2. The scope and extent,
3. Mitigating safeguards,
4. Residual risks, and
5. The specific duration

Each request shall be in writing to the VSU ISO and approved by the VSU Chief Information Officer (CIO) indicating the acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception, as well as, mitigating controls and all residual risks. The requesting data owner will be informed of the action taken. An exception will not be accepted for processing unless all residual risks have been documented. Denied exceptions may be appealed to the CIO of VSU. The form to document exceptions requests is included in Attachment A of this document.

Once the exception request is approved by the VSU CIO, the request is then submitted to the Office of the President of VSU for signature and submitted to VITA Commonwealth Security and Risk Management Office for final approval by the COY CISO.

Policy Review

This policy will be reviewed every two years on the anniversary of the policy effective date or more frequently as needs of the University warrants.

Violations of Policy

Violation of this policy may result in:

a. Disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4116/08, 611/11).

b. Prosecution under "Virginia Computer Crimes Act." § 18.2-152.1.

c. Loss of Information Technology usage privileges.

References

Virginia Information Technology Agency VITA):

Information Security Standard (SEC 501-09) (02/20/2015)

Approval By: _____ Date: 5/10/16

President