Privacy Policy for Employees' Electronic Communications

No. 7035

Policy Effective Date:
1/9/2015

Last Revision Date
11/27/2023

Policy Owner:
Sharon P. Pitt, Vice President for Information Technology and Chief Information Officer

Policy Author:
(Contact Person)
Brenda van Gelder, Executive Director, Information Technology Policy and Strategic Engagement

Affected Parties:
Faculty
Staff

1.0 Purpose

This policy defines the balance between the university's business needs, including information technology (IT) security requirements, and respect for employees' freedom of inquiry and expression with regard to electronic information and technology resources owned and provided to employees by the university.

2.0 Policy

Employees of Virginia Tech, which is a public university, are subject to the applicable laws and conditions of the Commonwealth. Therefore, employees should have no expectation of privacy with regard to university-owned data, infrastructure and technology resources.

In general, however, the university does not access or disclose the content of electronic information without the employee's consent. The university may access or disclose electronic information only for legitimate business purposes and will be limited to the minimum degree to accomplish the specified purpose.

2.1 Scope

This policy applies to all university technology resources and electronic information used, accessed, or produced by Virginia Tech employees of all types, including student and wage employees. Eligibility to access or use the university's electronic information services or technology resources is extended at the discretion of the university. Use of such resources serves as the user's consent to the procedures described herein.

Pursuant to the Acceptable Use Policy, the university owns, controls, and has a custodial relationship with respect to its electronic communication systems and certain classes of information stored on those systems including, for example, email containing university administrative data, communications pertaining to university business, operations, governance, and deliberative activities, and proprietary information. As a general matter, because such information is university property, employees should have no expectation of privacy in such data. Furthermore, such data are subject to the Freedom of Information Act as well as other federal and state laws and regulations.

2.2 Legal or administrative circumstances where access may occur without employee authorization are:

- communications or files required to be released by law, by orders of a court, or requested in accordance with the Virginia Freedom of Information Act;
- allegations of violations of law or policy that require investigation or documentation under university policy;

- approved Internal Audit reviews;
- prevention of cyber threats and resolution of technical problems;
- emergency situations involving an imminent threat of irreparable harm to persons or property; and,
- resources assigned to a group or publicly available to any user.

3.0 Procedures

Authorization for non-law-enforcement university personnel to access electronic information or files of employees will not be granted casually. Such authorization will require justification based on reasonable business needs or reasonably substantiated allegations of violation of law or policy on the part of the employee. In carrying out retrieval of files or information, due respect should be accorded to confidential or personal information and legally protected files.

Explicit consent never constitutes an intrusion. Employees may freely give consent to other individuals to access information stored on equipment or technology resources assigned to them. No further authorization is required in such instances.

3.1 Investigations of Violations of Law or Policy

Requests for authorization to access electronic information or files because of allegations of violations of policy or law by faculty or staff members may originate with supervisors. Requests must be made in writing and include the rationale for the request, a description of the information or files to be accessed or retrieved, and the proposed handling and disposition of the files. Authorization in such cases may be granted by the relevant senior manager or higher level authority, if needed.

The senior manager who is asked to consider authorization for accessing the electronic information or files of an employee must use his or her best professional judgment in determining if reasonable grounds exist, considering the surrounding circumstances and environment, to grant such authorization. The senior manager is expected to maintain confidentiality in such a situation. He or she may wish to consult with the Office of the General Counsel or Division of Human Resources in determining whether to authorize access or review, and in determining if the affected employee or anyone else should be notified that the access or review is taking place.

3.2 Business Needs

As stated in section 2.0 of this policy, the university may access or disclose electronic information only for legitimate business and will be limited to the minimum degree to accomplish the specified purpose. Where there is a reasonable need for access to routine business or educational documents and the employee is unavailable, authorization to access that employee's electronic information should be provided by the department head or director, or next higher authority. Whenever possible, the employee should be informed and asked to help in obtaining the needed business materials. If that help is not reasonably available, then other steps should be considered to respect the confidential or personal nature of any other materials present. Except in situations described in this policy, the employee will be promptly notified of the access and the nature of the documents or communications reviewed or obtained. Any such access is also governed by Policy 4082, Appropriate Use of Employee Personnel and Pay Records.

3.3 Reporting Requirements

During the processes above, university personnel may observe certain activity data or other electronic information that is beyond the scope of employee work. Except as provided elsewhere in this policy or by law, university personnel are not permitted to seek out such information, including contents or activity data, when not germane to system operations and support. If, in the course of their duties, university personnel inadvertently discover or suspect violations of law or university policy including the Acceptable Use Policy, such personnel have an obligation to report such violations to a department head or director, or next higher authority and may need to preserve the data for investigation. This exception does not exempt systems personnel from the prohibition against disclosure of personal or confidential information.

4.0 Definitions

Employees include all persons directly employed by Virginia Tech in their capacity as employees. The policy also covers anyone to whom the electronic communications and computing resources of employees have been extended. These include (but are not limited to) recently terminated employees whose communications and computing resources have not yet been terminated, deleted, or transferred, consultants that may be hired, and individuals whose electronic communications and computing resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who are using state-owned equipment and carrying out university work.

Technology resource – any item such as a computer, tablet, smartphone, server or similar device and associated peripherals owned by Virginia Tech or used to store university data, including those in cloud services and for research contracts or private activities associated with the university, and privately-owned technology devices that are connected to the Virginia Tech network or used to store university data.

5.0 References

Department of Human Resources Policy 1.75
http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf

Policy 4082, Appropriate Use of Employee Personnel and Pay Records.
https://policies.vt.edu/assets/4082.pdf

Virginia Freedom of Information Act Title 2.2, Chapter 37
http://law.lis.virginia.gov/vacode/2.2-3700/

Policy 7010, Policy for Security Technology Resources and Services
http://www.policies.vt.edu/7010.pdf

Frequently Asked Questions (FAQ About IT Security Monitoring
https://evpcoo.vt.edu/Initiatives/ittransformation/projects/cybersecurity/improved-endpoint-protection.html

Board of Visitors Resolution Approved March 20, 2023
https://bov.vt.edu/assets/Minutes-March%2019-20,%202023-30.pdf

Policy 7100, Administrative Data Management and Access Policy
http://www.policies.vt.edu/7100.pdf

Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
http://www.policies.vt.edu/7000.pdf

Acceptable Use Standard
https://vt.edu/acceptable-use.html

Policy 2000, Management of University Records
http://www.policies.vt.edu/2000.pdf

Policy 13000, Policy on Intellectual Property
http://www.policies.vt.edu/13000.pdf

Policy 5615, University Safety and Security
http://www.policies.vt.edu/5615.pdf

Policy 5617, Safety and Security Camera Acceptable Use Policy
https://policies.vt.edu/5617.pdf

Policy 5620, Access Control: Key Control Policy
https://policies.vt.edu/5620.pdf

Government Data Collection and Dissemination Practices Act, Sec. 2.2-3800 et seq.
http://law.lis.virginia.gov/vacode/2.2-3800/

6.0 Approval and Revisions

Information system technology is characterized by rapid evolution and the development of innovative, novel applications. It is the intent of this policy to establish basic principles that will endure through many evolutions of information systems.

The Vice President for Information Technology & Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed for consideration by university leadership.

Approved by the University Council on February 21, 2005
Approved by the President, Charles W. Steger, on February 21, 2005
Approved by the Board of Visitors on March 14, 2005

September 7, 2006: Technical revisions – (1) policy renumbered to Information Technology Policy 7035 from former General University Policy 2035; (2) references updated.

- Revision 1
  - Updates to hyperlinks throughout.
  - Section 3:1: "Equal Opportunity Office" and "Personnel Services" changed to "Department of Human Resources."

  Approved January 9, 2015 by Vice President for Information Technology and Chief Information Officer, Dr. Scott F. Midkiff.

- Revision 2
  - Updates to organizational structure
  - Updates of hyperlinks and references

  Approved November 21, 2019 by Vice President for Information Technology and Chief Information Officer, Dr. Scott F. Midkiff

- Revision 3
  Based on the BOV Resolution passed March 20, 2023 and due to the deployment of newly acquired IT security tools and processes required for the continually evolving data and systems security needs of the University, the policy was modified to provide transparency about the use of these tools and processes during routine operations for university employees. Accordingly, significant changes were made to sections 1, 2, and 3 of the policy. Employees may request more detailed information about these changes by contacting the IT Security Office at security@vt.edu.

  Approved November 27, 2023 by Executive Vice President and Chief Operating Officer, Amy Sebring.