
Subject: Appropriate Use of Electronic Personnel and Payroll Records

1. Purpose	1
2. Policy	1
2.1 Authorized Users	2
3. Procedures.....	2
3.1 Termination of Access.....	3
3.1.1 Process for Terminating System Access.....	3
3.1.2 Departmental Ability to Access an Employee's ID.....	3
3.1.3 Departmental Ability to Block an Employee's ID	3
4. Definitions	4
5. References.....	4
6. Approval and Revisions.....	4

1. Purpose

The intent of this policy is to define appropriate access to the Human Resources Information System (HRIS) and to set forth guidelines to safeguard the use and maintenance of personnel and payroll information.

2. Policy

University communication and computing resources are used to support the educational, research and public service missions of the institution. Activities involving these resources must be in accord with the university honor codes, employee handbooks, student handbooks and relevant local, state, federal and international laws and regulations.

For use to be acceptable it must demonstrate consideration for:

- the rights of others to privacy;
 - intellectual property rights (e.g., as reflected in licenses and copyrights);
 - ownership of data;
 - system mechanisms designed to limit access; and
 - individuals' rights to be free of intimidation, harassment, and unwarranted annoyance.
1. Employees must be authorized by their department head or documented designee and Human Resources for access to personnel and payroll data on the Human Resources Information System (HRIS). Only employees who need direct access to personnel and payroll data in order to perform specific job responsibilities should be given this authorization. Access should be limited to only the departmental data and information for HRIS forms and reports required to perform the duties of the job. Human Resources will provide HRIS training to new users as part of the authorization process.
 2. With the exception of requests for employment references, requests for personnel-related information from an organization or individual not associated with Virginia Tech *must be referred* to Human Resources. Address and phone information indicated as "confidential" on the HRIS cannot be released to individuals or organizations outside of the university.

3. Employees having access to personnel and payroll data must only use this information for job-related purposes—not for the personal use by others or themselves. It must only be shared with employees within their own department who need the information to perform their job responsibilities. [Policy 7100, Administrative Data Management and Access Policy](#), defines data users as *individuals who have need for university data in order to perform their assigned duties and are therefore authorized access*. All data users must sign a statement on the [Human Resource Information System \(HRIS\) Access Request Form 131](#) indicating their understanding of the level of access provided and their responsibility to likewise maintain the inherent privacy, accessibility, and integrity of the data they are provided.
4. Representatives of university departments whose official functions include audits or investigations may have inquiry access to records when access to data is needed for specific official investigations. Such access must be justified in writing to the Associate Vice President for Human Resources by the dean, director or department head of the requesting department for all audits and official investigations (such as the State Employee Fraud, Waste and Abuse Hotline) conducted by university departments.
5. The university regards any violation of this policy as a serious offense. Violators of this policy are subject to disciplinary action as prescribed in the undergraduate and graduate honor codes, and the student and employee handbooks.

2.1 Authorized Users

All employees requesting authorization must complete and sign the [Human Resource Information System \(HRIS\) Access Request Form 131](#) certifying they have read [Policy 4082, Appropriate Use of Electronic Personnel and Payroll Records](#), and [Policy 7000, Acceptable Use of Computer and Communication Systems](#), and that they agree to protect their access privileges accordingly. They must then obtain appropriate signature approval from the department head (or appropriate dean or vice president signature approval if for more than one department within a senior management area). No one may approve his or her own authorization; approval should always be at the next level of management.

Department representatives will have access to a limited amount of non-sensitive data for all university employees to assist them with employment-related tasks. This includes: an employee's name, identification number, department name and number, position number, employment dates, funding, and accumulated wage hours. Also included are data about completion date of I9 and visa status. Authorized departmental representatives can view salary information for employees only within their department.

Department head approval is required for access to the department data. Approval by deans/vice presidents or designees is required for access to one or more departments within a senior management area.

Senior management executives may have access to personnel and payroll data for all units reporting to them.

Access to university-wide data must be approved by the appropriate senior-level management, Provost or Vice President for Administrative Services, and the Associate Vice President for Human Resources or documented designee. Certain administrative offices (e.g., EOAA, Budget and Financial Planning) will have access to appropriate personnel and payroll data for all university departments and employees.

3. Procedures

1. All personnel and payroll information must be stored in a secure, confidential environment.

2. Owners of an access ID are accountable for its use. It is the ID owner's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information.
3. Passwords should never be displayed, printed or otherwise recorded in an unsecured manner.
4. Electronic IDs and passwords that provide access to HRIS must not be shared with other individuals. The new system provides audit trails of many electronic transactions and will record the ID used to enter or change data, thus making the owner of the ID accountable for any actions entered on the IDs. Therefore, workstations should always be attended while still connected to any HRIS system. This includes Banner HR, the HR web reports, and the leave system or any administrative information systems where data integrity or confidentiality may be compromised.
5. Anyone who has reason to suspect a breach of established security policy or procedure should promptly report it to the appropriate dean, director or department head and to the Computing Center, specifically the Information Resource Management (IRM) office.

3.1 Termination of Access

3.1.1 Process for Terminating System Access

Department heads at Virginia Tech authorize employees to have IDs on the various computer systems during employment; therefore, the department head is accountable for ensuring that employee access is blocked in situations where there are job changes, separations or transfers. To inactivate system access, IRM uses a daily report of personnel actions (separations, transfers, promotions, and demotions) that have been entered on Banner to determine which IDs need to have system access terminated. Timely processing of personnel actions assures timely termination of systems access.

The [Operational Policy for Individual Access to E-Mail/Modem Pool Accounts](#) states that all access, including email, belongs to the university upon employee separation.

3.1.2 Departmental Ability to Access an Employee's ID

A department head or designee may need immediate access to information under an employee's ID when the employee is separated unexpectedly or absent for a long period of time (i.e., handling payroll in a small department where there is no backup).

The department head or designee should send an e-mail message to IRMHELP@vt.edu listing systems to which the employee has access and request the IDs be set for access by an alternate ID or individual. For emergency situations, a phone call should be made to IRM (231-6716) after sending the email to ensure immediate action.

3.1.3 Departmental Ability to Block an Employee's ID

A department head or designee may need to block an employee from using their ID for the following reasons:

- when an employee is separated unexpectedly;
- when an employee is absent over a long period of time; or
- when an employee is a threat to the workplace.

The department head should send an e-mail message to IRMHELP@vt.edu listing systems to which the employee has access and request that the ID(s) be terminated by a certain date. In *these* cases, the ID is considered university property. For emergency situations, a phone call should be made to IRM (231-6716) after sending the email to ensure immediate action.

4. Definitions

Data Users: individuals who have need for university data in order to perform their assigned duties and are, therefore authorized access.

ID: Identification to access computer systems at Virginia Tech. The ID is assigned to an employee by Information Resource Management in the Computing Center. ID, PID, Oracle ID are interchangeable in this policy.

5. References

[Policy 7100, Administrative Data Management and Access Policy](#)

[Operational Policy for Individual Access to E-Mail/Modem Pool Accounts](#)

[Policy 7000, Acceptable Use of Computer and Communication Systems](#)

[Policy 2010, Release of Names and Addresses of Students, Faculty, Staff and Alumni](#)

Department of Human Resource Management, [Policy 1.60, Standards of Conduct and Performance](#)

6. Approval and Revisions

Approved September 8, 1999, by Assistant Vice President for Personnel, Linda Woodard.

October 10, 2001: Technical corrections to update policy links and name change for the Commonwealth of Virginia's Department of Human Resource Management (formerly Department of Personnel and Training).

September 7, 2006: Technical revisions to update references – (1) delete reference to obsolete Policy 2020: Policy on Protecting Electronic Access Privileges; (2) update reference to former Policy 2005 to current Policy 7100: Administrative Data Management and Access Policy; (3) update reference to former Policy 2015 to current Policy 7000: Acceptable use of Computer and Communication Systems; (4) Update to “Human Resources” all references to “Personnel Services.”

- Revision 1

May 13, 2008: Updates to position titles and/or responsibilities due to university restructuring.