TENNESSEE STATE UNIVERSITY
The Office of Human Resources

Computer Access – 6.10.2

---

**PURPOSE:**

This policy establishes restrictions regarding the access and use of University owned and maintained computers, computer systems, computer networks, electronic communications facilities, and other related computing facilities used to store and process data, text and software used by the University.

**POLICY**

It is the policy for the University to grant access to university owned computers and computer systems/networks with written authorization by system/network owners for actively engaged students, employees, consultants and other designated persons having a bona fide need to access information.

**PROCEDURES**

- Access to TSU networks and systems must be granted via a unique account(s) linked to a specific user.
- Access to University networks and systems should be granted only to users whose access is required to perform their job duties.
- Students are granted access to university networks and systems for purposes of registration, grades, account information and other uses necessary for them to matriculate.
- All network and system access must be approved by the user's supervisor and the data owner.
- Access must be terminated in a timely manner upon employee termination, change of job role, end of contract or service with vendor, or any other event that renders any part of the user's access unnecessary.
- The on-line ESA notification must be completed by the supervisor to notify the Office of Information Technology to disable user accounts in a timely manner.
- Permissions assigned to individual accounts, as well as groups / roles with permissions assigned to them, should be reviewed periodically by the user's supervisor or data owner to determine if the access remains appropriate and modified as needed.

- Banner Native Access must be temporarily terminated within 24 hours after the occurrence of the following circumstances:
  a. Three days of consecutive employee absence.
  b. On or before the first day of FMLA.
  c. Employee placed on any type of leave with or without pay, excluding vacation and holidays.
  d. Employees who appear to have abandoned their jobs (three days) before they receive a termination notice.
  e. Employees who have not worked for three consecutive days and keep calling in to extend time off.
  f. Employees who give or receive notice of separation and are permitted to stop working on that date.
  g. Retirees will have their computer access disabled on the last day of work even if they are receiving terminal leave.
- Employees will be allowed to maintain their email accounts while still an employee of the university, but not actively at work.
- Supervisors may request resumption of Banner Native Access by use of the same form by checking the appropriate information.
- Supervisors must maintain accurate attendance records and use the ESA notification to disable user accounts within twenty-four hour of non-attendance and use of annual or holiday leave has been granted.
- ESA notification will be part of the supervisor's annual performance evaluation.
- Non-compliance shall be documented by the supervisor and forwarded to the appropriate Vice President for review.
- Supervisors who fail to comply with the termination procedures shall be subject to progressive disciplinary action, including warnings, suspensions, and employment termination.
- Department and division heads are also subject to disciplinary actions when subordinates continue to be in non-compliance with the ESA notification guidelines.
- The University President will be provided a quarterly report of all employees who fail to comply with the ESA notification guidelines.

---

**REFERENCE**
OTS Security Policy

Adopted
Effective Date 11/01/2019

Glenda Glover

Dr. Glenda B. Glover, President Date