**IT Security Policy for Handling Departing Students' Accounts**

**Jason Browder**

**CS 4451 Computer Security**

**Professor David Tyson**

When students leave school before completing their programs, their digital footprints and account access must be handled carefully. If not managed properly, it can lead to security risks, data breaches, and even compliance violations (Easttom, 2024). As educational institutions increasingly rely on cloud-based technologies, having a clear and structured policy for handling departing students’ accounts is more critical than ever.

This policy safeguards institutional data and ensures a smooth and secure process for deactivating departing students’ accounts while complying with security best practices and legal requirements. This policy applies to all students who leave before completing their academic programs, whether due to withdrawal, expulsion, or other forms of termination.

**Policy Details**

**1. Notification of Departure**

* As soon as a student’s departure is confirmed, the Registrar’s Office must notify the IT department immediately.
* The notification should include the student’s full name, ID number, and departure date (Easttom, 2024).

**2. Account Deactivation**

* The IT team must deactivate the students’ digital access (ex., emails, portals, and any university-provided software accounts) within 24 hours of receiving the notification.
* Access should be revoked based on the principles of least privilege and implicit deny, ensuring that no unnecessary access remains active (Easttom, 2024; National Institute of Standards and Technology [NIST], 1995).

**3. Data Retention and Transfer**

* Student data should be securely archived or removed based on institutional policies and legal regulations (Lepide, 2023).
* If applicable, students must be allowed to transfer personal or academic files (e.g., research, assignments) before their accounts are deactivated.
* When cloud-based storage is involved, encryption and strict access controls must be used to prevent unauthorized access.

**4. Access to Physical and Virtual Resources**

* Any ID cards, access badges, or keys assigned to the student must be collected.
* Physical access to campus facilities, such as computer labs, research centers, and libraries, should be revoked immediately (Easttom, 2024).

**5. Security Audit and Documentation**

* A security audit must be conducted to ensure the departing student hasn’t engaged in unauthorized activities before their departure (NIST, 1995).
* The entire account deactivation process should be recorded and securely stored for compliance and future reference (Pathlock, 2023).

**6. Confirmation of Deactivation**

* Once all necessary steps have been completed, IT should send final confirmation to the Registrar’s Office and other relevant departments.

**7. Policy Review and Updates**

* This policy should be reviewed and updated periodically to stay aligned with evolving security threats and regulatory requirements.
* Feedback from IT audits, security reports, and compliance checks should be incorporated into updates (Pathlock, 2023).

**Supporting Guidelines**

* Data Classification and Protection: All student data should be handled in compliance with FERPA and internal security policies (Lepide, 2023).
* Incident Response Plan: IT should have a well-defined process for detecting and responding to security breaches during the account deactivation process (NIST, 1995).
* Staff Training and Awareness: IT personnel and administrators should be trained on best practices for secure account management (Easttom, 2024).

By implementing these measures, we can protect institutional data, maintain compliance, and ensure a secure transition for departing students.

**References**

* Easttom, C. (2024). *Computer security fundamentals* (5th ed.). Pearson Education.
* Lepide. (2023). *Tips to securely manage user accounts in higher education*. <https://www.lepide.com/blog/tips-to-securely-manage-user-accounts-in-higher-education/>
* National Institute of Standards and Technology. (1995). *An introduction to computer security: The NIST handbook* (Special Publication 800-12). <https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter10.html>
* Pathlock. (2023). *Deprovisioning: Best practices for removing user access*. <https://pathlock.com/learn/deprovisioning/>