TITLE: EU 1.21 Security Awareness Training Policy V1.0

Owner: Office of Information Technology
Approval: IT Security Council
Version: V1.0
Issue Date: 03/12/2018
Effective Date: 03/12/2018

Purpose:
Ivy Tech Community College of Indiana (ITCC) [1]Information Technology (IT) Systems are intended to promote the educational mission of the College. This entails the protection of ITCC [2]Institutional Data from the compromise of ITCC IT Systems by providing required Information Security Awareness Training (ISAT) to (ITCC) employees to help build their knowledge in identifying and mitigating the unauthorized access, processing, manipulating, or destruction of Ivy Tech Institutional Data and/or IT Systems.

Scope:
This Policy is intended for all current ITCC employees including but not limited to Students, Faculty, adjunct-faucly, Staff, or Affiliates, who have access to ITCC Institutional Data and IT Systems (Excluding Federal work-study students and Dual Credit Only Faculty).

Policy

Principle
All current ITCC employees who have access to [1]ITCC IT Systems and/or [2]Institutional Data are required to pass semi-annual ISAT consisting of multiple module, in a timely manner. Failure to comply with this policy will cause the ITCC employees ITCC accounts to be deactivated immediately after the ISAT deadline has passed. Completion of ISAT shall be monitored by ITCC Human Resources and ITCC employee account deactivation requests for ITCC employees who have not completed the ISAT shall be sent to ITCC Office of Information Technology (OIT) for ITCC account deactivation. To get a deactivated ITCC account activated, an account activation request must be sent to information Security from the ITCC employees regional HR Department. The ITCC employee then has three business days to complete the required ISAT. After the third reactivation request the ITCC employee will receive a formal written Performance Improvement Plan (PIP) from their immediate supervisor, further violation of this policy may cause the ITCC employee to lose their ITCC computing privileges, either temporarily or permanently, and could also face other disciplinary actions as outlined in the, Full-time/Part-time Employee Handbooks, and the Academic Support and Operations Manual.

Procedure
1. User receives an email from HELPDESK ALERT (ivyalerts.ivytech.edu) containing details about the next round of ISAT to the their ITCC employee Microsoft Outlook Email Account
2. User receives a seperate email from IvyLEAD (notifications@ivytech.bridgeapp.com) to the their ITCC employee Microsoft Outlook Email Account for each module in the current ISAT with a Web Link to one of the Training Modules and the ISAT due date.
3. Training is accessible through the College's Learning Management System, IvyLEAD or via the clicking the link in the emails from IvyLEAD
    a. To access IvyLEAD
        1. Log in to MyIvy using your ITCC employee account username and password
        2. Click the "EMPLOYEE" link on the left toolbar
        3. Click the "Employee Dashboard" link on the left toolbar
        4. Click on the IvyLEAD icon
4. Immediately after the stated due date in step 2, ITCC employees who have not completed the ISAT will have their ITCC employee accounts deactivated and will have no access to ITCC [1]IT Systems or [2]Institutional Data.
5. Users whose ITCC employee accounts have been deactivated will be required to personally contact their Regional ITCC HR Department for their ITCC employee account reactivation.

6. The ITCC employees Regional HR Department will contact ITCC Information Security to reactivate the employees ITCC accounts
7. ITCC Information Security will repond to to HR that the employees ITCC accounts have been reactivated via an email to the Regional HR representative and the ITCC employees Microsoft Outlook ITCC Account.
8. The ITCC employee has three business days to complete the ISAT
9. Failure to complete the ISAT in the time period allotted will cause the ITCC employees ITCC accounts to be deactivated again.
10. The ITCC employee then has to go through step 5 of this process again for ITCC accounts reactivation
11. After three employee ITCC account reactivations the ITCC employee will receive a formal written Performance Improvement Plan (PIP) from their immediate supervisor.
12. Continued failure to complete the required ISAT in the allotted time may incur other disciniplinary actions

Definitions

[1]**Information Technology (IT) Systems:** in regards to this policy; include all ITCC owned, licensed, or managed hardware and software, and any used by the ITCC network via a physical or wireless connection, regardless of the ownership of the device connected to the network, who have access to ITCC Institutional Data and IT Systems.

[2]**Institutional Data:** in regards to this policy; any data, records, or information owned by or entrusted to ITCC that ITCC creates, obtains, accesses (via records, systems, or otherwise), receives, processes, or uses in the course of ITCC's educational mission or business requirements which include, but not be limited to: social security numbers; C-Numbers; credit card numbers; any data protected or made confidential or sensitive by the Family Educational Rights and Privacy Act (FERPA), as set forth in 20 U.S.C. §1232g, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the federal regulations adopted to implement that Act (45 CFR Parts 160 & 164 "the HIPAA Privacy Rule"), the Gramm-Leach-Bliley Act (GLBA), Public Law No: 106-102, or the Release of Social Security Number Indiana Code 4-1-10. ITCC Data also includes all information, including personally identifiable information, derived from other ITCC records.

Referenced Documents

- **Full-time Employee Handbook**
- **Part-time Employee Handbook**
- **Academic Support and Operations Manual**