Information Security Awareness

SUBJECT:	Information Security Awareness Policy
REFER QUESTIONS TO:	Information Security Officer
EFFECTIVE DATE:	1/1/2016
APPROVED BY:	Trine University Executive Management
DISTRIBUTED TO:	Workforce Members

I. PURPOSE

Trine University has a responsibility in reference to security best practices, state, and or federal laws for providing and documenting security awareness and training for workforce members. Therefore, each workforce member can properly carry out their job function while protecting the 'Confidentiality, Integrity, and Availability' of Trine University's data assets.

II. SCOPE

This policy applies to all workforce members.

III. POLICY

Security Reminders

Trine University's Information Technology Department shall be responsible for taking steps to ensure that workforce members, including those who work remotely, receive security reminders periodically and as needed, including:

a. On information security risks and how to follow Trine University's information security policies and procedures

b. On how departmental managers or designated trainers will show workforce members how to use information systems and applications in a manner that reduces security risks, and on selected topics, including:

   i. Legal and business responsibilities of Trine University for protecting of data assets that reside on / in information systems and applications.
   ii. Signification of risks to Information Systems and applications that house data assets

c. Any of the following events occur:

   i. Substantial revisions are made to Trine University's security policies and procedures because of the following:

      - Changes to State and Federal Laws
      - Organizational changes
      - Acquisition and Mergers

   ii. Substantial new security controls are implemented at Trine University whether it be Administrative, Technical, and Physical controls.

   iii. Substantial threats or risks arise that could affect the confidentiality, integrity, and availability of data assets, this includes the following examples:

      - Virus
      - Phishing Attempts
      - Applications / Operating systems vulnerabilities (SQL Injection, Cross-site-Scripting, Buffer overflows)

Trine University's Information Technology Department will have the means of providing security information reminders and updates that may include, but are not limited to:

1. Email reminders
2. Digital Media/Posters
3. Tests/Quizzes
4. Screen savers
5. Logon messages

Security Training

The Information Technology Department will create a security training program that will require a high level of participation from workforce members of Trine University:

1. The Security Training will contain the following elements to increase security therefore enhance the Confidentiality, Integrity, and Availability of data assets:

   a. Administrative:
      i. Policies and procedures
      ii. Security incident reporting
      iii. Data classification
      iv. Understanding of information security when it concerns state, federal and legal statutes
      v. Why a security breach at Trine University could be dangerous and costly

   b. Technical:
      i. Log-in monitoring
      ii. Password & Users account management
      iii. Security Defense in Depth

c. Physical:

   i. Key code and access card management

   ii. Procedures of when in possession of corporate assets outside of Trine University, this can include:

      1. Laptops
      2. Phones
      3. Non workforce members accessing corporate assets

   iii. Office environmental: this can include:

      1. Office Doors
      2. Cabinets
      3. Recycle Paper
      4. Paper Shredding

2. New workforce members are required to complete mandatory security training within 7 days of hire.
3. Department Managers will be required with input from the Information Security Officer to train workforce members. Department Managers will be responsible to report training compliance to Human Resources by print or email.

IV. RESPONSIBILITIES

All workforce members are subject to this policy and their responsibilities are to uphold this policy to the highest degree possible

V. COMPLIANCE

Failure to comply with this or any other security policy will result in disciplinary actions as per the Employee Handbook.

VI. REVISION HISTORY

This policy is subject to revision in response to changes in technology or Trine University operational initiatives.

Version	Date	Author	Change Description
1	12/11/2015	Information Security Committee	Formatting changes and official document approved for publication