The University of Georgia

University of Georgia
Role-based Security
Model Training
Role-based Security Model

- Required training, education and/or awareness will be provided for executive leadership, faculty, staff, students, and IT Professionals. Each type of training will be aligned with the role expectations and responsibilities.
- Completion of training will be tracked and included in operational procedures.
- Training in security will be ongoing with new materials added as security requirements change and for new hires.

Role-based Security Model

- IT Professionals
  - SANS training required for all staff in IT Jobs classification
    - SANS documents course completion
  - Phase II – Required and Recommended Training available through SANS, Element K, and UGA developed training (ITMF and other IT professionals)
  - UGA facilitated training for targeted groups (such as recent SANS boot camp)
  - Business Continuity, Incident Response, Security Liaison, Role-based Security Implementation for Managers/IT Leadership – Developed by UGA and available through Training and Development
Role-based Security Model

- Faculty and Staff
  - Phase I - Introduction to UGA Role-based Security Model
    - Expectations and requirements based on role
      - Required “Security in the Workplace” introduction
      - Description of future training modules tied to MYID password update
        - Process will capture completion of modules and will be required before password can be updated
  - Phase II – Modules of education/training developed for faculty and staff – Team led by College of Education
    - Modules 3 to 5 minutes addressing security
    - Email, Phishing, FERPA, File Sharing, Sensitive Data, Passwords, Policy, Virus Protection, etc.
    - Modules delivered via web to meet training requirements for MYID password refresh
  - Ongoing – Updates to resources and materials on Security Website to support model

Role-based Security Model

- Students
  - Phase I - Introduction to UGA Role-based Security Model
    - Expectations and requirements based on role
      - Required “Information Security for Students”
      - Description of future training modules tied to MYID password update
        - Process will capture completion of modules and will be required before password can be updated
  - Phase II – Modules of education/training developed for faculty and staff – Team led by College of Education
    - Modules 3 to 5 minutes addressing security
    - Email, Identify Theft, FERPA, File Sharing, Copyright, Passwords, Policy, Virus Protection, etc.
    - Modules delivered via web to meet training requirements for MYID password refresh
  - Ongoing – Updates to resources and materials on Security Website to support model
Role-based Security Model

• Students
  • Phase III – Security materials included in packet for New Student Orientation (added to safety information for physical security) This work will be a partnership with Student Affairs
  • Bookmarks, Posters in dorms, Information added to Student Computer Support site

Role-based Security Model

• Key contributions:
  • Approval of UGA Role-based Security Model by EMT
  • CIO and CISO
    • Role-Based Security Model – Executive Leadership 2/13/08
    • Role-based Security Model – Deans 2/2008
  • Meeting with ITMF – CIO and CISO 1/10/08
  • Development of application for notification of training modules, tracking of completion tied to MYID password refresh - EITS
  • Phase I – Communication/Introduction to model for faculty, staff, students (Workplace Security for Faculty and Staff and Information Security for Students – Available via security website)
  • Development of training modules for students, faculty and staff that will be required upon password refresh: Team of developers led by College of Education, Sandi Glass and Peter Norris (will seek instructional designers from other units)
  • PR campaign – Posters, bookmarks, website – (items available for download to units for local printing)
Role-based Security Model

Key contributions:

- ITMF:
  - Communication to all IT Professionals via units
  - Training
    - Development of training module to be offered by members of ITMF through Training and Development to cover:
      - Hiring qualified professionals (IT Matrix, Training requirements by role
      - Role and responsibilities of Security Liaison
        - Assets Management Tool
        - Resources at UGA to provide assistance in building secure systems
      - Incident Response Process
      - Security policies at UGA
      - Disaster Recovery Planning
      - Effective communication with Deans, Faculty, Staff and Students
      - Use of Security Resources (Web-site, training, etc.)
  - Letter of support for model
  - Advocacy

Role-based Security Model

Final Thoughts:

- Security awareness, education, and training will be ongoing (not a project with an end)

- We will create systems that document that training has been completed

- We will build in training as part of normal operations (MYID refresh, student orientations, professional groups/meetings on campus (ITMF, UGANet, Dean's meetings, Department meetings, etc.)

- We will develop focused training that is appropriate to the role of the individual (faculty, staff, student, IT Professional)

- Faculty, staff and student training/education/awareness are not intended to be adequate for individuals responsible for development, design, or administration of systems with sensitive data