Information Security Office
Project Updates

A Presentation to the IRCC
October 22, 2014

Jack McCoy, EdD
Director, Information Security Office
Projects

• ISO 27002
• Information Security Policies
• IT Risk Management
• User Awareness and Education
ISO 27002: Information Security

• Includes 114 controls (27002:2013)
• To be used as a basis for developing “organization specific” information security standards and guidance
• Some 27002 controls may NOT be applicable to an institution
• Selection of controls to be based on institutional risks, compliance requirements, contractual obligations
Information Security Regulation

• Defines individual responsibility for information security
• Defines management responsibility for protecting information in the care of their departments
• PRR request submitted, scheduled with University Policy Committee meeting on 11/25
Acceptable Use Policy

• Defines acceptable use of University IT resources
• Current policies do not address new challenges in our current technology environment
  – e.g. mobile and personally owned computing
• PRR request submitted, scheduled with University Policy Committee meeting on 11/25
ISO 27002: Information Security

• Internationally-recognized standard for information security management that provides *guidelines* for:
  – organizational information security controls and
  – information security management practices
IT Risk Management

• Annual IT Risk Assessment
• Compliance assessments (e.g., HIPAA)
• Adoption of risk management practices in IT decision making
• Integration into Enterprise Risk Management
User Awareness and Education

• Periodic reminders via newsletters and CIO tips
• SANS Securing the Human videos
• Core work values
• Featured events, such as National Cyber Security Awareness Month promotions
Stay Safe Online!
Visit www.staysafeonline.org for the latest cyber security tips…