The Information Security Practice Principles

1. **Comprehensivity:** Am I covering all of my bases?
   Identify and account for all relevant systems, actors, and risks in the environment.
   Related concepts: Complete Mediation, End-to-end Encryption, Reconnaissance, Inventory

2. **Opportunity:** Am I taking advantage of my environment?
   Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.
   Related concepts: Information Sharing, White Hat Testing, Deception, Common Tools

3. **Rigor:** What is correct behavior, and how am I ensuring it?
   Specify and enforce the expected states, behaviors, and processes governing the relevant systems and actors.
   Related concepts: Governance, Requirements, Monitoring, Audits

4. **Minimization:** Can this be a smaller target?
   Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.
   Related concepts: Attack Surface, Compactness, Data Minimization

5. **Compartmentation:** Is this made of distinct parts with limited interactions?
   Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes.
   Related concepts: Modularity, Forward Secrecy, Least Privilege, Air Gapping, Cryptography

6. **Fault Tolerance:** What happens if this fails?
   Anticipate and address the potential compromise and failure of system elements and security controls.
   Related concepts: Resilience, Failsafe Defaults, Defense in Depth, Revocability

7. **Proportionality:** Is this worth it?
   Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.
   Related concepts: Risk Management and Acceptance, Usability

CENTER FOR APPLIED CYBERSECURITY RESEARCH
PERVASIVE TECHNOLOGY INSTITUTE

For more resources, visit: *cacr.iu.edu/principles*

About the Principles Project

High-level principles underlie a great deal of existing information security practice, but these principles have remained under-researched and largely unarticulated in favor of highly detailed, prescriptive artifacts (e.g., NIST RMF, DIACAP, CIS Critical Security Controls, ISO, HIPAA security rule).

These artifacts may be loaded with great advice, but are difficult to understand without the benefit of significant prior training. They do little to help someone learn to think like a security practitioner or address novel, emergent situations.

The ISPPs provide a mental model for problem solving: They can be used to teach new or non-practitioners (e.g., students, executives) about information security; they can help practitioners make decisions in novel situations (where an established best practice may not exist); and they can add validity and salience to more detailed statements of best practice.

Project Team

Craig Jackson (*scjackso@iu.edu*) is the chief policy analyst at CACR, where his research interests include information security program development and governance, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defenses. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and leads CACR's collaborative efforts with Naval Surface Warfare Center Crane Division.

Scott Russell (*scolruss@iu.edu*) is a senior policy analyst with CACR, where his work focuses on the improvement of federal cybersecurity standards. A lawyer and researcher, Scott specializes in privacy, cybersecurity, and international law, and his past research has included cybersecurity due diligence norms under international law, cybersecurity self-governance, international data jurisdiction, and constitutional issues on digital surveillance.

Susan Sons (*sesons@iu.edu*) is the chief security analyst with CACR, and president of the Internet Civil Engineering Institute. She serves as information security officer of Open Science Grid, and advises the DHS-funded SWAMP project in operational security and software engineering. Susan's work and research focus on the security and safety of critical infrastructure software in scientific, ICS/SCADA, and core internet applications.

About CACR

The Indiana University Center for Applied Cybersecurity Research (CACR, *cacr.iu.edu*) is distinctive in addressing cybersecurity from a comprehensive, multidisciplinary, hands-on perspective. The Center draws on Indiana University's scholarly expertise in computer science, informatics, accounting and information systems, criminal justice, law, regulatory compliance, organizational behavior, and public policy.

Founded in 2003, CACR's recent work includes research awards from DHS, DOE, NSF, and collaborations with NSWC Crane Division, the Indiana National Guard, the City of Chicago, and Indiana's legal community. CACR leads the National Science Foundation's Cybersecurity Center of Excellence. Under CACR's coordination, NSA and DHS designated IU a National Center of Academic Excellence in Cyber Defense Research and Information Assurance/Cybersecurity Education. CACR is affiliated with the IU Pervasive Technology Institute.