# The Information Security Practice Principles

The Indiana University Center for Applied Cybersecurity Research

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 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*

# About the ISPP Project

The Indiana University Center for Applied Cybersecurity Research

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 normative 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, and 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 Chief Policy Analyst at CACR, where his research interests include information security program development and governance, legal and regulatory regimes' impact on information security, resilience, and innovative defenses. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and is on the security team for the DHS-funded Software Assurance Marketplace (SWAMP). He is a graduate of the IU Maurer School of Law and IU School of Education. In addition to his litigation experience, Craig's research, design, project management, and psychology background includes work at the IU Center for Research on Learning and Technology and the Washington University in St. Louis School of Medicine.

**Scott Russell** 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. He received his B.A. in Computer Science and History from the University of Virginia, received his J.D. from Indiana University, interned at MITRE, and served as a post-doctoral fellow at CACR.

**Susan Sons** is a software engineer and information security analyst dedicated to securing systems and software critical to our physical infrastructure, the Internet, computational science, and scientific research. Her work includes the rescue of the Network Time Protocol reference implementation, security operations on DHS-funded SWAMP and DOE/NSF-funded Open Science Grid projects, advising the GPS daemon project, and serving as a member of the NSF's Cybersecurity Center of Excellence. Susan is a Senior Systems Analyst at CACR.

**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 by now-IU President Michael McRobbie 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.