Security Plan
The executive heads of major University organizations are responsible for managing the risks associated with their assets. They must document and implement an Information Security Plan (Security Plan) that demonstrates due care in securing their assets by meeting the intention of the controls in Administrative Policy Statement 2.6.

Purpose
- Describe critical assets that support the organization’s mission
- Describe existing security controls
- Describe lines of responsibility and accountability
- Describe objectives and goals related to security and privacy

Goals
- Improve informed decision-making and prioritization of organizational efforts
- Help everyone understand the information environment
- Help everyone understand responsibilities and expectations
- Prepare for incident response
- Understand organizational and University-wide risks
- Comply with Administrative Policy Statement 2.6

Getting Started
Important considerations when developing a Security Plan:
- **One size does not fit all** – Some departments within a large organization or some individual assets may require their own Security Plan. Specific regulatory requirements, different IT environments, certain data types, critical business functions, and organizational reporting lines are some of the factors to consider when determining the approach that is best for your Security Plan.
- **Reference centralized services** – Rather than explain how centralized services (e.g. UW IT hosted server) work, it is sufficient to describe what particular requirements are addressed by centralized services, lines of responsibility, and how accountability is tracked.
- **Reference outsourcing** – Like centralized services, outsourcing solutions can be incorporated into the security plan by reference and with a description of how decisions are made about the third-party services.
- **Map asset dependencies** – An asset may be critical because of its own value or because other assets depend on it.
- **Use existing sources** – Leverage documentation, information resources, and systems that already exist.

Resources
The Office of the CISO has developed a “How-to” guide in order to ease the development, maintenance, and use of a Security Plan by drawing upon both the business and technical expertise that already exists within an organization in order to make security planning activities more natural.

Security Plan How-to Guide (docx)
Asset Discovery - Critical Info Systems (xls)
SECURITY PLAN “HOW-TO” GUIDE

The “How-to” guide suggests an approach and format that is meant to be generally helpful; the guide format is not a requirement or a template.

I. PLAN OVERVIEW
   a. PURPOSE AND SCOPE

II. ORGANIZATIONAL PROFILE
   a. MISSION AND VISION
   b. ORGANIZATIONAL STRUCTURE
   c. PROGRAM AND SERVICES

III. INFORMATION ASSETS SUMMARY
   a. CRITICAL DATA SUMMARY
   b. INFORMATION TECHNOLOGY SYSTEMS SUMMARY
   c. OTHER INFORMATION ASSETS

IV. DUE CARE STRATEGY
   a. SECURITY PHILOSOPHY
   b. INFORMATION SECURITY AND PRIVACY RISK
   c. EXISTING CONTROLS/EXISTING SECURITY ARCHITECTURE
   d. SECURITY INITIATIVES

V. APPENDICES
   a. DETAILED ASSETS
   b. DETAILED CONTROLS
   c. ADDITIONAL REFERENCES

1 The profile section answers the broadest questions about the “who” and “why” of an organization. It is helpful to lay out the relationship between the mission of an organization, the vision of leadership for how to pursue that mission, and the organization’s programs and services implementing that vision.

2 The asset summary gets into the “what” questions of an organization’s security risk management. The idea of Critical Information Assets need not be limited to hardware and software. Processes, personnel know-how, and the actual body of compiled data itself may overlooked as “assets” outside of an information security context because they are accounted for in ways that seem to lack formal maturity or copious documentation. Nevertheless, these overlooked “assets” often have the qualities of being surprisingly robust, long-standing, and critical to the organization.

3 The due care strategy is the “how” of security risk management. The security philosophy connects the business drivers of the organization to the priorities for safeguarding data and privacy. The information risk sections explore the known hazards that threaten to compromise those priorities. The existing security controls & architecture explores what is already being done to address those risks. The security initiatives describe future efforts to improve controls.