PURDUE
UNIVERSITY

Created by Purdue University NSF # 1840043

OFFICE OF INFORMATION TECHNOLOGY – SECURITY & POLICY

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI**):**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.3. General Description/Purpose of System: What is the function/purpose of the system?
[Provide a short, high-level description of the function/purpose of the system.]

1.3.1. Number of end users and privileged users: **[In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]**

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list. [**Document the CUI information types processed, stored, or transmitted by the system below**].

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. **[Insert the reference/URL or note that the hardware component inventory is attached.]**

2.2. List all software components installed on the system. **[Insert the reference/URL or note that the software component inventory is attached.]**

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain:]**

3. REQUIREMENTS

The Universities Security/Policy Office and Internal Audit collaborated in generating the consolidated controls to create an information security program. Controls are applied to research involving controlled unclassified information (CUI).

Source Special Publication: NIST Special Publication 800-171 Rev. 1, dated December 2016.