

IT Project Security Initial Review Form

Project Title:	Project Number:
Project Leader/Manager:	Anticipated Project Start Date:
Sponsor:	Date Prepared:

The security information for project management of information technology projects has two forms, this **IT Project Security Initial Review Form** and the **IT Project Security Final Review Form**. The purpose of this initial review form is to think about and document the security of the requested categories for this information technology project. The initial review form is completed and approved by the appropriate project personnel and the IT Security Office during the project planning process. See ["Instructions & Definitions"](#) for guidance.

This form applies to: the entire project, or component of the project Name of component:

Category	Required?	Provided by?	Comment/Description/Explanation
	Explain if No or N/A	(Vendor or In-house)	
1. Authentication and Authorization			
2. Encryption			
a. In Transit			
b. In Storage			
3. Handling Sensitive Private Data			
4. Regulatory Compliance			
5. Data Steward Info	Data Custodian Group:		
	Where Will Data Be Stored:		
	Describe Vendor Access:		

IT Project Security Initial Review Form

Category	Required?	Provided by?	Comment/Description/Explanation
	Explain if No or N/A	(Vendor or In-house)	
6. Will updates, patches and backup follow standard production operating procedures?			
a) Application			
b) Operating System			
c) Database, etc.			
d) Hardware			
e) Backups			
7. Physical Location	Is the hardware located in: <input type="checkbox"/> AISB Data Center <input type="checkbox"/> or CNS Switch Room? <input type="checkbox"/> if neither, give location & describe environmental condition below		
	Location:		
	<input type="checkbox"/> Access Controlled	Type Access:	<input type="checkbox"/> Environmentals Monitored <input type="checkbox"/> HVAC <input type="checkbox"/> UPS
8. Project Information: (Information needs to be complete enough so someone who is unfamiliar with the project can conduct a summary review.)			

IT Project Security Initial Review Form

Comments:

Approvals:

Duplicate or delete signature blocks as needed.

Requested by:

(e.g., project manager)

Printed name, Signature, Date

Approved by:

(e.g., project sponsor)

Printed name, Signature, Date

**Approved by
IT Security Office**

Printed name, Signature, Date

I. Determine Security Needs for Project:

Information Technology (IT) projects must be reviewed for potential security vulnerabilities throughout the project lifecycle. The IT Project Security Initial Review Form is used to assist in this review and for documenting any known issues and status.

The project manager determines which of the categories in the Security Worksheet are relevant for the proposed project, and if a review is necessary for the project as a whole or perhaps for individual components within the project. If the project involves the procurement of hardware or software from a vendor, consultation should be sought from the IT Security Office during the definition and evaluation phases of the procurement.

Project managers are encouraged to be familiar with security tools and analysis available from:

The IT Security Office, including lab testing. (see <http://www.security.vt.edu/>)

External agencies such as SANS. (see <http://www.sans.org/>)

Top 20 Internet Security Attack Targets. (see <http://www.sans.org/top20/>)

Open Web Application Security Project (OWASP) for web application security tests. (see http://www.owasp.org/index.php/OWASP_Top_Ten_Project)

Category Definitions:

1. Authentication and Authorization: Authentication is the process of verifying the identity of a user. Authorization is the process of establishing a user's rights or privileges to access the software/hardware associated with this project.

2. Encryption: Encryption is a process of converting data to a form that is incomprehensible utilizing an algorithm, so that the data can be reconverted only by an authorized recipient (human or machine). Data should be encrypted **In Transit** and while **In Storage** (at rest).

3. Handling Sensitive Private Data: Does the project process or store sensitive, private (nonpublic) data? Personally Identifying Information (PII)?

See Virginia Tech Policy 1060 and 7025 for details. (see <http://www.policies.vt.edu/index.php>)

See Virginia Tech Standard for Storing and Transmitting Personally Identifying Information (see <http://www.it.vt.edu/administration/policies/>)

4. Regulatory Compliance: If a vendor is involved in the project, are their components compliant with Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI), etc? For example, vendors providing credit card processing systems must be PCI compliant. Vendors should be able to produce letters of compliance upon request.

References:

[Virginia Tech Registrar information on Family Educational Rights and Privacy Act \(FERPA\)](#)

[Family Educational Rights and Privacy Act \(FERPA\)](#)

[Health Insurance Portability and Accountability Act \(HIPAA\)](#)

[Gramm-Leach-Bliley Act \(GLBA\)](#)

[Payment Card Industry \(PCI\)](#)

5. Data Steward Info: "University directors (typically at the level of Controller, Registrar, or Director of Admissions) who oversee the capture, maintenance and dissemination of data for a particular operation. Data Stewards are appointed by the respective Data Trustee. Data Steward responsibilities include the data management activities outlined in this policy and other activities that may be assigned by a Data Trustee."

[See Virginia Tech Policy 7100](#)

[See Virginia Tech Standard for administrative data management](#)

Data Custodian Group: Specify the university group responsible for the data.

Where Will Data Be Stored: Specify where the data is stored.

Describe Vendor Access: If a vendor is involved in the project, what rights/access (if any) do they have to the data?

I. Determine Security Needs for Project: (continued)

6. Updates, Patches, and Backups: Who is responsible for updating the project's software (operating system, application, and database) and hardware? Are updates performed in a timely manner? What checks are in place to ensure that updates and patches are indeed being applied? If a vendor is involved, what (if any) updates do they provide the project's software and hardware? Updates and patches apply to application software, operating system software, database software, system support software, hardware, etc. Ensure that the data is properly backed up for an up-to-date recovery and specify who is responsible for backups.

[See Virginia Tech Policy 7010](#)

7. Physical Location: The facility that houses the IT resources. What type of access controls, security systems, fire suppression systems, etc. are employed to protect the structure?

8. Project Information: Provide a brief synopsis of the project or attach the project initiation form.

Responses:

1. Required? Is the feature required for the project?

2. Provided By? Is the security feature provided in a vendor product or service being purchased as part of the project? Or, is the security feature provided by code developed by local staff or services supported by local staff?

3. Comment/Description/Explanation. Use this space to provide an appropriate explanation - specifically if the answer was No or N/A to any of the above.

II. Directions For Use:

1. Complete the IT Project Security Initial Review form.

2. E-mail the completed worksheet to the IT Security Office (ITSO@vt.edu).

3. The IT Security Office and project manager may schedule a security review of the project . The security review may be iterative.

4. Approval of the initial security components of this project are required from the IT Security Office before the project planning process is complete. Final approval of the projects security components are required from the IT Security Office, before production implementation.

See IT Project Security Final Approval form for more information.

5. Use form information as appropriate to complete the project scope form.

6. If desirable, attach the completed form to the project scope form.

7. Store completed form with the other project management documentation in the project document repository.

NOTE:

1. Carefully review the project to determine when the IT Security Office should become involved. For projects with software procurements, have the IT Security Office review security specifications early in the project lifecycle and before purchase is made. A hardware security review is required before production implementation.

III. Conclusions to be drawn from the Security Initial Review Form:

1. This is not a review of the project implementation. It is a review of the proposed security plan.
2. This form identifies security areas that must be addressed in the project.
3. This form identifies the security areas where the IT Security Office may want to conduct a more detailed review.
4. This form identifies who (vendor or VT) is implementing what.
5. As an initial review, this form does not necessarily define or evaluate how a project component is implemented. That is documented in the Security Final Approval form.