

# Information Access and Protection Plan FAQ

Updated 12/16/05

**General | Information Inventory | Protection by Media Type | Reuse, Retirement, Destruction | Human Protections | Next Steps**

## General

Q: What prompted this exercise?

A: It was prompted by the Gramm-Leech-Bliley Act (GLB) and other federal and state mandates. The first step towards compliance with GLB is completion of the information inventory.

Q: What exactly is the plan that needs to be in place? Is it the spreadsheet we've been working on or is this just something to help us brainstorm? It seems like the actual plan is the action items.

A: The completed spreadsheet is usable as your department's plan. It is a combination of existing safeguards and practices and action items identified by your department. The plan captures how you handle information and can help identify gaps in current practices.

Q: What does the plan do exactly?

A: The plan basically captures how you handle the information and can help to catch any problem areas in your process. It helps to identify gaps that may exist in your current protection process.

Q: Does this plan just help us determine the minimum acceptable levels of information protection?

A: Yes, it helps determine minimum level. Departments are encouraged to develop information handling best practices they can share with other departments.

Q: Where can I obtain a copy of the workshop presentation?

A: It is available from the IAP Resource Center at <http://security.rit.edu/iap.html>.

Q: Where can I find best practices for information handling?

A: RIT best practices are available from the IAP Resource Center at <http://security.rit.edu/iap.html>. For questions about specific items please contact Jim Moore at [infosec@rit.edu](mailto:infosec@rit.edu).

Q: I do not understand some of the technical safeguards in Part 2 of the Plan Template. Where can I get more information?

A: Contact Patrick Saeva or any other manager in ITS.

Q: If we have already done a preliminary plan for information we handle do we need to redo it to fit the formatting of the provided template?

A: No, the plan already done can be attached to the template. There is no need to redo it.

Q: Which organizational unit must create a plan?

A: Each department is responsible for creating a plan. However, it may be advantageous to combine plans with other departments or as a higher level organizational unit, if information handling is consistent across the departments.

Q: What is the timeline for putting the plan in place and will it be monitored?

A: The plan must be completed by December 15, 2005. Although we will not monitor each department's plan completion, you are required to furnish your plan to the Information Security Office upon request.

Q: Do the action items identified in the plan have to be completed by December 15, 2005?

A: You're not expected to have your action items completed by December 15<sup>th</sup> but all action items should be identified and a plan of action in place by December 15<sup>th</sup>.

Q: What if there is something not covered by the checkboxes on the template?

A: Feel free to make adjustments to the existing checkboxes to accommodate the practices of your department or add the information in the Comments section.

## ***Part One: Information Inventory***

### **Classification**

Q: Where can I find information about how specific types of information that should be classified?

A: Review the Information Classification Matrix in the IAP Resource Center.

Q: Does the standard include paper records as well as electronic?

A: It covers all media that confidential information is stored or recorded on.

Q: I know a student's name itself is not usually confidential, but at what point does it become confidential information?

A: When it is associated with other information that can be used to obtain access to private or confidential information, when it is associated with information that can be used to enable identity theft, when it is associated with other information such as grades that may be protected by legislative mandates, such as FERPA.

Q: With the switch over to student ID numbers from SSNs what happens if someone finds out both a student's name and their ID? Can there be internal identity theft? Under what level of security should these numbers be kept?

A: The new ID numbers will allow access to financial services, records information, etc., and should be treated as RIT Confidential.

### **Authoritative Source**

Q: Is the authoritative source box a yes/no answer?

A: Yes, it is asking if you are the authoritative source.

Q: Doesn't the classification for the information depend on the authoritative source?

A: The authoritative source should determine the classification for its information. However, in the absence of published classifications, each department should use their best judgment in determining the appropriate level of classification. Another alternative would be to contact the authoritative source and ask how the information should be classified.

Q: What do I do about information that seems to be owned by more than one department?

A: Communicate with the person completing the other department's IAP Plan to ensure consistent handling and agreement on information ownership.

Q: Does jointly-owned information need to be included in both departments' plans?

A: Yes. You must include jointly-owned information in both plans.

Q: If data is taken from many sources and compiled in a single report, which is the authoritative source for the information?

A: The owners of the data are the authoritative source for the data. However, the producer of the report is responsible to ensure that recipients of the report understand the confidentiality of the data contained in the report.

### **Handling**

Q: What is my department's responsibility when we receive information from another RIT source?

A: You are responsible for applying the appropriate safeguards to ensure the information is handled properly. When you pass RIT information on to another department, you must ensure the receiving department knows the appropriate data classification. These safeguards must be included in your plan.

Q: How do we ensure recipients of our information handle the information properly?

A: You can not ensure the recipients handle the information properly. Your responsibility is to communicate to them how the information should be handled.

Q: Is there a process for surrendering of confidential information such as in a subpoena?

A: Direct it to Campus Safety who deals with these more often and can evaluate the subpoena and get legal advice from Nixon Peabody.

Q: Does the plan require me to identify with whom information is shared?

A: No, that information is not required.

## ***Part Two: Protection by Media Type***

### **Relationship of Parts One and Two**

Q. What is the difference between Parts One and Two?

A. Part one is primarily concerned with classification of information. Part two is concerned primarily with how that information is stored or transferred.

Q: Do you complete an IAP Plan Part II page for everything listed in Part I?

A: No, we're looking for how the information is typically handled. You can talk about exceptions in the Comments field.

### **Information Storage**

Q: Do I fill out a separate section for each server or desktop (IAP Plan Part 2/3)?

A: We encourage you to complete each section based on a typical server or desktop. Discuss exceptions in the Comments field.

Q: If information is maintained on an internal department website, is it on the internet?

A: Yes, it is on the internet. Access restrictions to the internal department website may be noted in the Comments field.

## ***Part Three: Reuse, Retirement, Destruction***

### **Document Retention**

Q. Does RIT have a Document Retention/Destruction Policy

A. Not at this time. Departments are encouraged to use their best judgment when disposing of information.

## ***Part Four: Human Protections***

### **NDA**

Q: What is an NDA?

A: An NDA (Non-disclosure agreement) is a signed agreement in which the signer agrees to follow the information handling procedures detailed in the NDA.

Q: Is an NDA used only for RIT staff and faculty?

A: No, it can be used with anyone that handles the information.

## ***Part Five: Next Steps***

### **Action Items**

Q: We've found several procedures that we need to develop or change. What do we do now?

A: Use the Action Items section to include information about changes that must be made.

### **Plan Maintenance**

Q: We've made the changes we listed as Action Items. When do we update the Plan?

A: Although the IAP Plan requires review at least every two years, we encourage you to make updates to the Plan and you make changes to your procedures.