1 Access Control Policy

1.1 Overview

The owner of an information asset will first consider the relevant business, legislative, and statutory security requirements and then determine the access restrictions to be placed on that asset. The policy of least privilege access will be adopted as the default approach in all cases; that is, "access is generally forbidden unless expressly permitted." These restrictions will be characterized by an access classification category. An access classification will be used to implement the administrative, technical, and operational controls that are appropriate to safeguard the information. A set of standard general access and operating system-specific controls applicable to nearly all Xyz information assets is specified in later sections of this document. Additional controls may be specified by the Computing Security Team for new implementations as part of the system development lifecycle (SDLC) information security risk management process. For new information assets established as part of the SDLC, the Technical Project Manager assigned by the Project Management Office is accountable for the initial implementation. Accountability for the on going administration and sustainment of those access controls is handed off to the appropriate operational support teams once the system is launched. These same operational support teams are accountable for maintaining the general access and OS-specific controls.

1.2 Information Assets Ownership

A list of enterprise information assets and the related owners is included as Appendix A to this document. The listed owner or a delegate shall establish the access restrictions for that information asset.

1.3 Information Asset Access Classification

The classification of new information assets is accomplished as part of the system development lifecycle as defined in the *[ISO A.3.3] SDLC Information Security Risk Management Process* document. In most cases this will involve a data security review by the Computing Security Team that will document the information security asset classifications made by the asset owner. A list of these access classification categories follows and applies to all information assets regardless of media. The intent of this document however is specifically to define the policies, processes, and logical controls for digitized data that is being transported, stored, or processed. The requirements for labeling and handling hardcopy documents and removable media are contained in the *[ISO A.10] Media Management* document.

The following information asset access classifications shall define the access granted to that asset:

- **Individual**

  Access/distribution restricted to the data owner.

- **Limited Group**

  Access/distribution restricted to a department or team.

- **Internal**

  Access/distribution restricted to within Xyz.

- **Limited External**

Access/distribution restricted to within Xyz and specifically designated partners or contractors.

- **External**

  No access restrictions.

1.4 Information Asset Access Controls

Once an information asset has been classified, the appropriate controls must be implemented to enforce the specified level of access. The “General Access Controls” and “Operating System Access Controls” that pertain to most Xyz information assets follow. Additional controls may be imposed on new assets as part of the system development life cycle though. For those assets, consideration will also be given to levels of confidentiality, integrity, availability, and accountability defined by a business system or service owner. In these cases, Computing Security will use the *[ISO A.3.3] SDLC Information Security Risk Management Process document* to specify any additional controls needed. These additional controls will be listed in the system documentation. The Technical Project Manager assigned by the Project Management Office is accountable for ensuring that the specified access controls are implemented. Accountability for the on going administration and sustainment of these access controls is then handed off to the appropriate operational support teams. These same operational support teams are accountable for maintaining the general access and OS-specific controls defined in the following sections.

---

10. Classifying Your Work Products

10.1. (ISP 7.2.1)

Were all information workers who create products like specifications, source code, architectural diagrams, project plans, spreadsheets and so forth. Yet not all of these "information assets" that we create are intended for access by or distribution to everyone in the world, right? The vast majority of them are intended for Xyz employees only but there is also information that is only meant to be shared with specific partners, customers, or even just within certain teams. So how does a creator of information define these access limitations in common terms that everyone can understand? It's a simple three step process:
Decide who should and should not be able to access the information in question based on its value, legal requirements, sensitivity and criticality to Xyz.
Select a "data access and distribution classification" (listed below) that matches this access.
Tack on a set of "handling instructions" (examples below) to clarify exactly who should have access. We have found that words like "Xyz confidential" (don't use this!) are weak and ambiguous and so we came up with an official classification scheme that literally tells you who is allowed to read it!

10.2. (ISP 10.2)

That's all there is to it. If you need them, detailed classification guidelines are contained in the *[ISO 10.2] Access Control* Policy document. In general though, the following list of our classifications probably gives you enough guidance to handle most situations:

- Individual. This is the most restrictive access classification. Literally, this means only the owner of the data has access to it. Every employee in this company owns data in this classification -your user account password! Another example of data to which this might apply is proprietary information from another company that is being shared in an extremely limited fashion with one of our business unit people for deal negotiation. A typical document security label (including handling instructions) might read

"Individual --Proprietary & Confidential Data: Access or distribution limited to Joe Smith."

- Limited Group. This access classification limits distribution of data to within a specific team or department. An example of data to which this might apply is a table of customer credit card numbers existing on a product database to which access must be restricted to all but a subset of specifically designated system administrators or DBAs. A typical document security label (including handling instructions) might read " *Limited Group -- Proprietary & Confidential Data: Access or distribution limited to Windows System Administrators."*
- Internal. Access to data in this classification is restricted to employees of Xyz. An example of data to which this might apply is the project plan for a new product. "Internal" is the most common data security classification in our company. A typical document security label (including handling instructions) might read *"Internal -- Proprietary & Confidential Data: Access or distribution restricted to Xyz employees."*
- Limited External. This access classification limits distribution of data to the employees of Xyz and those specifically designated partners or contractors for which there exists a compelling business justification for that access. An example of data to which this might apply is a description of the network implementation for a specific Xyz product that has been requested by a partner for a contractually defined security audit. A typical document security label (including handling instructions) might read " *Limited External-- Proprietary & Confidential Data: Access or distribution restricted to Xyz employees and to partners or contractors specifically designated by the VP, Product Engineering."*
- External. This is the least restrictive access classification. Literally, this means anyone in the world can have access to the data. An example of data to which this might apply is a press release that announces a business relationship with a new customer. A typical document security label (including handling instructions) might read *"External -- Public data: No restrictions on access or distribution."*

So now you're an expert on the required method of classifying the information you produce! In the next two pages of the User's Guide, we'll talk about how to use these classifications for communicating sensitive information and labeling media.

11. Communicating Sensitive Information (ISP 10.8.1)

So, what information is considered sensitive? Simply, it is any information that has an information security access classification of "limited external," "internal," "limited group," or "individual." Sensitive information carries with it certain responsibilities for all those who handle it. These responsibilities are detailed in the [ISO A. 10.8.1J