**IT Department  
Policy, Standards, and Operations Guide**



**Prepared By**

|  |  |
| --- | --- |
| **Document Owner(s)** | **Project/Organization Role** |
|  |  |
|  |  |
|  |  |

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Section 1. IU IT-Related Policies 4](#_Toc309826112)

[IT-01: Appropriate Use of Information Technology Resources 4](#_Toc309826113)

[IT-02: Misuse and Abuse of IT Resources 4](#_Toc309826114)

[IT-03: Eligibility to Use IT Resources 4](#_Toc309826115)

[IT-07: Privacy of Electronic Information and Information Technology Resources 4](#_Toc309826116)

[IT-11: Excessive Use of IT Resources 4](#_Toc309826117)

[IT-12: Security of IT Resources 4](#_Toc309826118)

[IT-18: Network and Computer Accounts Administration 4](#_Toc309826119)

[IT-19: Extending the University Data Network 4](#_Toc309826120)

[IT-20: Wireless Networking 4](#_Toc309826121)

[IT-21: Use of Electronic Mail 4](#_Toc309826122)

[ISPP-24: Web Site Privacy Notices 5](#_Toc309826123)

[ISPP-25: Information Governance 5](#_Toc309826124)

[DM-01: Policy for Management of Institutional Data 5](#_Toc309826125)

[Section 2. Departmental IT Policies 6](#_Toc309826126)

[Subsection A. Computer and Mobile Devices Support Policy 6](#_Toc309826127)

[Subsection B. Computer and Server Replacement Cycle Policy 6](#_Toc309826128)

[Subsection C. Computer Access Security and ePHI Policy 6](#_Toc309826129)

[Subsection D. Encrypted Flash Drive Policy 6](#_Toc309826130)

[Subsection E. Multifunction Copier Policy 6](#_Toc309826131)

[Subsection F. Remote Access to Systems by Vendor Policy 6](#_Toc309826132)

[Subsection G. Windows 7 Upgrade Policy 6](#_Toc309826133)

[Subsection H. Restriction of Administrative Level Access Policy 6](#_Toc309826134)

[Subsection I. Et Cetera 6](#_Toc309826135)

[Section 3. Compliance with IU Policy, System Administrators Guidelines 7](#_Toc309826136)

[Subsection A. IU Policy IT-07 7](#_Toc309826137)

[Subsection B. IU Policy IT-12 8](#_Toc309826138)

[Subsection C. IU Policy DM-01 11](#_Toc309826139)

[Section 4. Compliance with IU Policy, Developers Guidelines 12](#_Toc309826140)

[Subsection A. IU Policy DM-01 12](#_Toc309826141)

[Section 5. Standard Operating Procedures 17](#_Toc309826142)

[Subsection A. IT-SOP-01-Infrastructure Password Change Procedures 17](#_Toc309826143)

[Subsection B. IT-SOP-02-Server Patching Procedure 17](#_Toc309826144)

[Subsection C. IT-SOP-03-Client System Patching Procedure 17](#_Toc309826145)

[Subsection D. IT-SOP-04-System Compromise Procedure 17](#_Toc309826146)

[Subsection E. IT-SOP-05-System Refresh Procedure 17](#_Toc309826147)

[Subsection F. IT-SOP-06-Employee Termination Procedure 17](#_Toc309826148)

[Subsection G. IT-SOP-07-Server Security Scanning Procedure 17](#_Toc309826149)

[Subsection H. IT-SOP-08-Equipment Surplus Procedure 17](#_Toc309826150)

[Section 6. Security and Privacy Principles 18](#_Toc309826151)

[Section 7. Disaster Recovery Preparedness 20](#_Toc309826152)

# Section 1. IU IT-Related Policies

All employees are required to abide by all IU policies. Employees engaged in information technology should pay particular attention to policies IT-07, IT-12, and DM-01.

The full list of IT-related policies is linked here. Each is also available online at <https://policies.iu.edu/information-it/index.html>. This portion of the document will be reviewed once each year to ensure that all policies are listed.

## [IT-01: Appropriate Use of Information Technology Resources](https://policies.iu.edu/policies/it-01-appropriate-use-it-resources/index.html)

## [IT-02: Misuse and Abuse of IT Resources](https://policies.iu.edu/policies/it-02-misuse-abuse-it-resources/index.html)

## [IT-03: Eligibility to Use IT Resources](https://policies.iu.edu/policies/it-03-eligibility-use-it-resources/index.html)

## [IT-07: Privacy of Electronic Information and Information Technology Resources](https://policies.iu.edu/policies/it-07-privacy-it-resources/index.html)

## [IT-11: Excessive Use of IT Resources](https://policies.iu.edu/policies/it-11-excessive-use-it-resources/index.html)

## [IT-12: Security of IT Resources](https://policies.iu.edu/policies/it-12-security-it-resources-current/index.html)

## [IT-18: Network and Computer Accounts Administration](https://policies.iu.edu/policies/it-18-accounts-administration/index.html)

## [IT-19: Extending the University Data Network](https://policies.iu.edu/policies/it-19-extending-data-network/index.html)

## [IT-20: Wireless Networking](https://policies.iu.edu/policies/it-20-wireless-networking/index.html)

## [IT-21: Use of Electronic Mail](https://policies.iu.edu/policies/it-21-use-email/index.html)

## [ISPP-24: Web Privacy Notices](https://policies.iu.edu/policies/ispp-24-web-privacy-notices/index.html)

## [DM-01: Policy for Management of Institutional Data](https://policies.iu.edu/policies/dm-01-management-institutional-data/index.html)

# Section 2. Departmental IT Policies

## Subsection A. Computer and Mobile Devices Support Policy

Paste your policies here, or reference their location. You might consider noting how often these policies are reviewed, and who must sign off on them. The policies listed here are found at the IT Policy Compliance SharePoint Site (http://xxx.xxxxxxx.edu/xxx)

## Subsection B. Computer and Server Replacement Cycle Policy

## Subsection C. Computer Access Security and ePHI Policy

## Subsection D. Encrypted Flash Drive Policy

## Subsection E. Multifunction Copier Policy

## Subsection F. Remote Access to Systems by Vendor Policy

## Subsection G. Windows 7 Upgrade Policy

## Subsection H. Restriction of Administrative Level Access Policy

## Subsection I. Et Cetera

# Section 3. Compliance with IU Policy, System Administrators Guidelines

## Subsection A. IU Policy IT-07

The purpose of this section is to map each requirement of policies IT-07, IT-12, and DM-01 to specific actions taken by your IT department. Be sure to keep it up-to-date and to formalize an approval process.

|  |  |  |  |
| --- | --- | --- | --- |
| Require-ment ID | Description | Action | Result |
| IT-07.2 | Stored electronic files and voice and data network communications may not be accessed by someone other than:   * the person to whom the account in which the information has been stored is assigned; or * the person from whom the communication originated, or to whom the communication was sent; or * the person to whom the device containing the stored electronic files has been assigned; | The ADS permissions on all users’ personal home directory on the server will set in the following manner:  SYSTEM: R  ADS\DeptAdmin: Full Control  ADS\UserName: RWM  Permissions on shared folders will never allow an account other than an Admin account to have full control. All permissions to shared folders will be handled via group membership. No individual permissions are allowed. | All user data is better protected, and audits of security permissions are easier to manage. |
| IT-07.3 | A technician or administrator may access or permit access to specific information technology resources and electronic information as defined in this policy, in [certain] circumstances… | Any access to a user’s personal folder, or a group’s shared folder, for \*any\* reason must be logged in the “Log Book” on [\\servername\folder\file](file:///\\servername\folder\file). Notification must also be made to the owner of the folder and the IT Manager of this department. | Compliance with IT-07 is maintained and there is better transparency for the department. |

## Subsection B. IU Policy IT-12

All personnel with administrative access to any server, workstation, laptop, or network-accessible device (e.g., systems) must adhere to the procedures set forth in this document. The following requirements apply to all systems, at all times, and are described in the “Policy Compliance Checklist” located at <http://abcdef.iu.edu>. The “Requirement ID” in the left column refers to the requirements listed in that document.

|  |  |  |  |
| --- | --- | --- | --- |
| Require-ment ID | Description | Action | Result |
| IT-12.2.4 | Remove or disable unneeded services and software, especially those that are network-accessible. | Join the system to ADS and move computer object to OU IU-DEPT-1234 in order to apply Group Policy IU-DEPT-GPO1234 | Group Policy IU-DEPT-GPO1234 is configured to meet this requirement |
| IT-12.2.5 | |  | | --- | | Log activities on the system: | | 1.    Successful user logins, including the location from which the logins originated, | | 2.    Unsuccessful login attempts, including the location from which the attempts originated, | | 3.    Unsuccessful file access attempts, and | | 4.    Successful file accesses for files and databases containing sensitive information. | | Join the system to ADS and move computer object to OU IU-DEPT-1234 in order to apply Group Policy IU-DEPT-GPO1234.  In addition, all servers will run **[name your log monitoring agent]** so that logs can be easily monitored. | Group Policy IU-DEPT-GPO1234 is configured to meet this requirement |
| IT-12.2.6 | Disable or secure remote access from system-to-system (e.g., rlogin). | Join the system to ADS and move computer object to OU IU-DEPT-1234 in order to apply Group Policy IU-DEPT-GPO1234 | Group Policy IU-DEPT-GPO1234 is configured to meet this requirement |
| IT-12.2.7 | Proactively seek out and apply vendor-supplied fixes necessary to repair security vulnerabilities… | Visit the [Information Security website](https://informationsecurity.iu.edu/security-bulletins/index.html) to discover updated vendor information.  All system administrators must subscribe to the UISO bulletins listserv. [Click here for instructions.](https://kb.iu.edu/d/bczz) | Information on important patches and updates will be delivered via e-mail. |
| IT-12.2.7 (continued) | …within a timeframe commensurate with the level of risk (i.e., within 24 hours for high-risk, with 48 hours for medium-risk, and within 72 hours for low-risk). | Based on advice and information from UISO, vendors, and other reliable sources, security vulnerabilities should be applied to production systems within a timeframe described in policy IT12. When feasible, fixes should first be tested on non-production systems. | Systems are protected from security threats. |
| IT-12.2.10 | Deploy encrypted communications methods (e.g., Secure Shell) for user access to the system and for access via privileged accounts (e.g., "root") from other than the console. | Only **[name your encrypted communications program]** shall be used to access systems remotely; when off campus, VPN shall be used in addition to **[name your encrypted communications program**]. | Systems are better protected from “man in the middle” and other attack vectors. |
| IT-12.2.11 | Technically limit access to local network addresses where possible (e.g., TCPWrappers) given the function or process being supported. | Join the system to ADS and move computer object to OU IU-DEPT-1234 in order to apply Group Policy IU-DEPT-GPO1234. | Group Policy IU-DEPT-GPO1234 is configured to meet this requirement. |
| IT-12.2.12 | |  | | --- | | Scan computers for security vulnerabilities using available technical tools: | | 1. Regularly, at least every 30 days to ensure new vulnerabilities are identified promptly, | | 2. Immediately after installation/configuration of a new system is completed, | | 3. Immediately after introduction of a new operating system or an upgrade to a current operating system, and | | 4.  Immediately after installation or upgrade of networking or other system software. | | The system administrator of **[name your patch management system]** shall verify on a weekly basis that scans are running and all computers are within the scope of scans being performed.  All technicians shall immediately initiate security updates after a new system is installed, upgraded, or networking or other system software is installed or upgraded (i.e., Windows Update) | Systems are better protected from hackers, exploits, and other attack vectors. |
| IT-12.2.13 | Install and maintain anti-virus software on operating systems for which Indiana University has licensed such software, and maintain current virus pattern files. | All systems, including servers, will have anti-virus software installed.  The system administrator of **[name your anti-virus console]** shall verify that all systems are receiving updated virus patter files or are configured to download virus pattern files automatically. | Systems are better protected from viruses and other malware. |
| IT-12.2.14 | Subscribe to vendor and other advisory services applicable to the operating environment being maintained. | Visit the [Information Security website](https://informationsecurity.iu.edu/security-bulletins/index.html) to discover updated vendor information.  All system administrators must subscribe to the UISO bulletins listserv. [Click here for instructions.](https://kb.iu.edu/d/bczz) | Information on important patches and updates will be delivered via e-mail. |
| IT-12.2.15 | Periodically visit the web site of the ITSO to view current bulletins or to obtain recent security guides and other related material. | Visit the [Information Security website](https://informationsecurity.iu.edu/security-bulletins/index.html) to discover updated vendor information.  All system administrators must subscribe to the UISO bulletins listserv. [Click here for instructions.](https://kb.iu.edu/d/bczz) | Information on important patches and updates will be delivered via e-mail. |
| IT-12.2.16 | Provide access to only those persons who are otherwise eligible to use Indiana University technology resources… | If an external person (such as a consultant, temporary employee, or support engineer) requires access to any system, an affiliate account must be requested. |  |
| IT-12.2.16 (continued) | …and require all users be identified and authenticated before access is allowed. | Access to any system must always require credentials; auto-logon is not allowed. |  |
| IT-12.2.17 | Limit access to needed services to only authorized persons. | Authorization from the proper data steward (Student Services Director, or Office Manager, for example) is required before access to data or systems is granted. |  |
| IT-12.2.18 | Use different passwords for privileged accounts ("root", for example) on various systems being maintained by the same technician(s). | No duplicate passwords should be used on various systems; each system should have a unique root/admin password. | Systems are better protected, since a cracked or hacked password on one system will not grant access to other systems. |
| IT-12.2.19 | Perform day-to-day work as a non-privileged user and only use privileged accounts for tasks that require additional capabilities. | System administrators will request a secondary ADS account for privileged use, while using their primary account for normal activities and tasks that don’t require administrative access. | Security risks are reduced. |
| IT-12.2.20 | Ensure that all accounts require a password, and if technically possible, that there are automatic routines (dictionaries, pattern enforcers, etc.) that force the user to choose a good password initially and each time the password expires. | Where possible, passwords will be at least 14 characters long. On a system where that is not possible, complex passwords (mixing upper and lower case, special characters) will be used. | Systems are better protected from cracking attempts. |
| IT-12.2.21 | Implement a system such that all re-usable passwords are not sent over the network in clear-text, where technically possible. | Encrypted all data traffic to and from systems using SSL certificates or IPSec. | Systems are better protected from passwords being intercepted. |
| IT-12.2.22 | Securely remove data from media once that data and/or device is no longer required, in order to prevent unauthorized disclosure of the data. | *List or link to your procedures for wiping personal computer hard drives, server hard drives; destroying optical media; removing data from PDA’s and other portable devices.* | Risk of critical or limited-access data exposure is reduced. |

## Subsection C. IU Policy DM-01

|  |  |  |  |
| --- | --- | --- | --- |
| Require-ment ID | Description | Action | Result |
| DM-01.4.6 | Unattended workstations with access to directories containing limited-access data must be logged off, locked, or otherwise made inaccessible to individuals without access rights. Where technically feasible, this equipment must be set up for automatic lock-out after 15 minutes of non-use. | Join the system to ADS and move computer object to OU **IU-DEPT-1234** in order to apply Group Policy **IU-DEPT-GPO1234** | Group Policy **IU-DEPT-GPO1234** is configured to meet this requirement |
| DM-01.4.11 | Limited-access data must never be stored on individual user workstations, laptops, personal digital assistants (PDA), or any other type of electronic equipment. Limited-access data must be stored on registered, and properly configured and managed, department or central file servers. | Always properly inform users of the proper location to store institutional data.  Protect all servers with a hardware firewall. | Data is more secure, and the risk of exposing data is decreased. |
| DM-01.4.17 | If institutional data are stored on any component of the university information system, that system component must have defined a formal system administration function and have assigned to it a system administrator whose responsibilities include: physical site security; administration of security and authorization systems; backup, recovery, and system restart procedures; data archiving; capacity planning and performance monitoring. | See Sections **X, Y, and Z** of this document.  In addition, all servers must be protected by a hardware firewall.  All backup media must be encrypted. | Systems and data are more secure, reliable, and available. |
| DM-01.4.18 | University servers that are used to store limited-access data must comply with specific management standards, as outlined in IT-12, issued by the University Information Policy Office. Web and other servers that must be accessible from off-campus must be physically separated from servers hosting limited-access institutional data. | In consultation with developers, data users, and others, determine which servers host limited-access data and keep them separate from web and other servers accessible from off-campus.  In addition, all servers must be protected by a hardware firewall. | Systems and data are more secure. |
| DM-01.4.19 | Direct access to university file servers hosting limited-access institutional data must be blocked from non-IU network addresses. Individuals requiring direct access to files stored on these servers from off-campus must first connect through the university’s modem pool or (preferably) the IU virtual private network (VPN) service. | On-campus systems which do not require access to the Internet must be assigned private IP addresses. This includes, but is not limited to, printers, file servers, print servers, and servers hosting intranet applications. | Systems and data are more secure. |

# Section 4. Compliance with IU Policy, Developers Guidelines

## Subsection A. IU Policy DM-01

All personnel who develop applications must adhere to the procedures set forth in this document. The following requirements apply to all systems and all critical and limited-access data, at all times, and are described in the “Policy Compliance Checklist” located at <http://abcdef.iu.edu>. The “Requirement ID” in the left column refers to the requirements listed in that document.

This document is to be reviewed at least once each year. Changes to this document should be vetted through the IT Director.

|  |  |  |  |
| --- | --- | --- | --- |
| Require-ment ID | Description | Action | Result |
| DM-01.4.1 | Applications that capture and update institutional data must incorporate edit and validation checks to assure the accuracy and integrity (consistency) of the data. | During database development, appropriate input masks, default values, and other validation rules should be applied; all such rules should be documented. | Data accuracy and integrity is increased. |
| DM-01.4.4 | All data extracted or reported from institutional data must include a record or display of the time and date of data capture. | All such transactions should be logged, including the userID of the person initiating the request, the date and time, and the action (read, edit, add, delete). Logs should be kept for a minimum of 2 years. | Logs are useful for troubleshooting and auditing purposes. |
| DM-01.4.5 | All data users having access to limited-access institutional data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of the data they access. | Perform an automated check against the Acceptable Use Agreement database to ensure users have assented. | Doing so ensures that policies and procedures put in place by data stewards and managers are not circumvented. |
| DM-01.4.7 | Individuals requiring access to central sources of restricted institutional information must be authorized by the appropriate data steward or manager and subsequently must use the UITS Decision Support Service (DSS) via the IU Information Environment (IUIE) for that access. | Appropriate checks must be put in place such that users who have not been authorized by the appropriate data steward or manager do not have access to institutional data. | Doing so ensures that policies and procedures put in place by data stewards and managers are not circumvented. |
| DM-01.4.8 | Where technically feasible, the IU central authentication service (CAS) must be used for all services that facilitate update or inquiry access to limited-access data on university servers. | Additional development time will be allowed to accommodate this requirement. | A more integrated and secure environment is achieved. |
| DM-01.4.9 | Where technically feasible, password tokens (in addition to secure password) must be required for any update access to restricted institutional data on university servers. | Additional development time will be allowed to accommodate this requirement. When reviewing a peer’s code, this requirement should be specifically noted in the accompanying report. | Systems are more secure. |
| DM-01.4.10 | Departments (including UITS and its regional campus counterparts) must eliminate insecure protocols for connecting to all university systems, and for transferring data to and from those systems, especially those servers that support critical operations and/or host limited-access data. | Data must always be encrypted in transit, using either SSL certificates or IPSec. | Systems and data are more secure. |
| DM-01.4.11 | Limited-access data must never be stored on individual user workstations, laptops, personal digital assistants (PDA), or any other type of electronic equipment. Limited-access data must be stored on registered, and properly configured and managed, department or central file servers. | Additional development time will be allowed to accommodate this requirement, in order to verify that data is not cached locally and to develop safeguards against downloading information to one’s computer. Any cached data must be encrypted, then purged when no longer needed. | Data is more secure, and the risk of exposing data is decreased. |
| DM-01.4.13 | When limited-access university data are stored on appropriate servers, they must not include SSNs unless they are keys to linking with other files. | DO NOT store SSN’s, unless specifically required by law or absolutely necessary for business functions.  Additional development time will be allowed to accommodate this requirement. When reviewing a peer’s code, this requirement should be specifically noted in the accompanying report. | The risk of exposing critical data is decreased. |
| DM-01.4.14 | SSNs must not be collected from individuals nor extracted from central systems and stored on departmental servers unless doing so is absolutely required to maintain the business functions of the office involved. | Before creating a field for SSN's, make triple sure it is functionally required and there are no alternative methods of achieving the same goal. | The risk of exposing critical data is decreased. |
| DM-01.4.15 | So that standards for survey research and FERPA requirements for non-directory student records are met, all program evaluation and assessment data must be stored in such a way that responses are not associated with individual names or SSNs. Linkage files containing the association of protected data to individuals must be placed in different directories and with different naming conventions to obscure the connection, and must be permanently deleted when no longer needed. | Use your own unique identifier system to track surveys, and keep the translation table in another location.  Additional development time will be allowed to accommodate this requirement. When reviewing a peer’s code, this requirement should be specifically noted in the accompanying report. | The risk of exposing critical data is decreased. |
| DM-01.4.16 | A student may file a directory exclusion to prevent disclosure of public information. For this reason, student public information must not be stored on local servers unless updated daily. | Use real-time access methods when possible.  Additional development time will be allowed to accommodate this requirement. When reviewing a peer’s code, this requirement should be specifically noted in the accompanying report. | The risk of exposing critical or limited-access data is decreased. |
| DM-01.4.18 | University servers that are used to store limited-access data must comply with specific management standards, as outlined in IT-12, issued by the University Information Policy Office. Web and other servers that must be accessible from off-campus must be physically separated from servers hosting limited-access institutional data. | Close consultation with system administrators is needed to ensure that this requirement is met. | Systems and data are more secure. |
| DM-01.4.19 | Direct access to university file servers hosting limited-access institutional data must be blocked from non-IU network addresses. Individuals requiring direct access to files stored on these servers from off-campus must first connect through the university’s modem pool or (preferably) the IU virtual private network (VPN) service. | Close consultation with system administrators is needed to ensure that this requirement is met. In some cases, IP filtering may be an option. | Systems and data are more secure, and the risk of data exposure is decreased. |

# Section 5. Standard Operating Procedures

## Subsection A. IT-SOP-01-Infrastructure Password Change Procedures

Paste your policies here, or reference their location. You might consider noting how often these policies are reviewed, and who must sign off on them. The policies listed here are found at the IT Policy Compliance SharePoint Site (<http://xxx.xxxxxxx.edu/xxx>)

## Subsection B. IT-SOP-02-Server Patching Procedure

## Subsection C. IT-SOP-03-Client System Patching Procedure

## Subsection D. IT-SOP-04-System Compromise Procedure

## Subsection E. IT-SOP-05-System Refresh Procedure

## Subsection F. IT-SOP-06-Employee Termination Procedure

## Subsection G. IT-SOP-07-Server Security Scanning Procedure

## Subsection H. IT-SOP-08-Equipment Surplus Procedure

# Section 6. Security and Privacy Principles

The principles defined here are taken from IU’s Security & Privacy Program principles, located at: <https://privacy.iu.edu/privacy-matters/principles.html>, which should be monitored periodically for updates and changes.

This section is to be reviewed by all IT staff at least once each year. Changes to this document should be approved through the IT Director.

|  |  |  |  |
| --- | --- | --- | --- |
| **Core Principles** | | | |
| Confidentiality Principle | Only authorized individuals have access to information. |
| Integrity Principle | Information must be reliable and accurate (sometimes referred to as the Quality Principle). |
| Availability Principle | Information must be available when needed. |
| **Additional, More Specific Security & Privacy Principles** | | | |
| Accountability Principle | Accountability and responsibility for the security and privacy of information must be clearly defined and acknowledged (sometimes referred to as the Management, Administrative Requirements, or Responsibility Principle). |
| Awareness Principle | Members of the university community must be aware of principles, [standard](http://protect.iu.edu/glossary/10#term651)s, conventions or mechanisms for maintaining the security and privacy of information. |
| Ethics Principle | Information is to be used, and security and privacy goals are to be executed, in an ethical manner. |
| Multidisciplinary Principle | Security and privacy governance must address the considerations and viewpoints of all interested parties (sometimes referred to as the Democracy Principle). |
| Proportionality Principle | Security and privacy [safeguards](http://protect.iu.edu/glossary/10#term658) are to be proportionate to the risks. |
| Integration Principle | Security and privacy design and implementation are to be coordinated and integrated within the system of safeguards and the life of the [information asset](http://protect.iu.edu/glossary/10#term678) (sometimes referred to as the Security Management Principle or the Security for Privacy Principle or the  Security Safeguards Principle). |
| Timeliness Principle | Parties will act in a timely and coordinated manner to prevent or respond to breaches of and threats to security and privacy. |
| Assessment Principle | Risks to information are to be assessed initially, and reassessed periodically. |
| Equity Principle | The rights and dignity of individuals are to be respected while carrying out security and privacy goals (sometimes referred to as the  Fairness Principle). |
| Notice Principle | Informs the individual about privacy policies and [procedure](http://protect.iu.edu/glossary/10#term650)s and identifies the purposes for which the individual's information is collected, used, disclosed and retained (sometimes referred to as the Purpose Specification or the Openness Principle). |
| Choice & Consent Principle | Obtains implicit or explicit consent from the individual with respect to the collection, use, disclosure and retention of the individual's information, particularly if that information is to be used for a secondary purpose or disclosed to a [third party](http://protect.iu.edu/glossary/10#term676) (sometimes referred to as the Objection Principle). |
| Collection Limitation Principle | Collects only the information needed to achieve the purposes identified by the business unit in support of the university's mission, and as outlined in the notice. |
| Use & Retention Principle | Uses the individual's information only as outlined in the notice, and keeps the information only as long as necessary to fulfill the stated purposes. |
| Disclosure Principle | Discloses the information to third parties only as outlined in the notice and as consented to by the individual either implicitly or explicitly. |
| Access Principle | Provides access to the individual to review and update or correct his or her information (sometimes referred to as the Participation Principle). |
| Monitoring & Enforcement Principle | Monitors compliance and has procedures to address complaints and disputes (sometimes referred to as the Recourse or the Redress Principle). |

# Section 7. Disaster Recovery Preparedness

Description of this section goes here.

Attach, or link to, your disaster recover/business continuity plan. It is best practice that each decision maker in your department have a hard copy of your DR/BC plan. For more information, visit <https://informationsecurity.iu.edu/resources-professionals/disaster-recovery-planning.html>.