



The New 14 Information Security Policies
Coral Gables Campus

FAQ

➤ Business Continuity Disaster Recovery (A135)

Questions:

1. What is business continuity disaster recovery planning?
2. Why is business continuity disaster recovery planning important?
3. How do I get started with business continuity disaster recovery planning in my area?
4. Who do I contact for with additional questions about the policy and/or for further assistance?

Answers:

1. Business continuity includes all activities performed by an organization to ensure that critical business functions will be available as expected. This includes all activities performed daily, weekly, monthly, quarterly, etc. to ensure consistency of service and recoverability.
2. Business continuity disaster recovery procedures and processes are an essential component for every information technology environment to ensure data and resources are recoverable in the event of any interruption.
3. The following supplemental materials are intended to assist an IT organization document and establish appropriate disaster recovery plans and procedures ([Click here to access the supplemental documents](#)).
4. For questions about the policy and/or additional assistance contact the Chief Information Security Office at ciso@miami.edu.

➤ Cardholder Information Security (A140)

For any questions regarding new or existing credit card processes contact the Executive Director of Treasury Operations, Hiram Sem at 305-284-5237 or via email: hsem@miami.edu.

➤ Change and Incident Management (A145)

Questions:

1. What is change and incident management?
2. Why is change and incident management important?
3. How do I get started with change and incident management in my area?
4. Who do I contact for with additional questions about the policy and/or for further assistance?

Answers:

1. Change management is a structured approach to managing the transition from a current state to a future state. Incident management refers to the activities an organization engages in to identify, analyze and correct issues as they arise.

2. Establishing appropriate change and incident management processes will minimize the risk of unexpected downtime and issues associated with unplanned, untested changes and/or implementations.
3. The following supplemental materials are intended to assist and IT organization document and establish appropriate change and incident management plans and procedures ([Click here to access the supplemental documents](#)).
4. For questions about the policy and/or additional assistance contact the Chief Information Security Office at ciso@miami.edu.

➤ Hardware Repurposing and Decommissioning (A150)

Questions:

1. If I receive a new computer, does my old system have to be sanitized even if it goes to another employee within my same department?
2. Who do I contact for sanitizing storage media?
3. My department has some systems we wish to donate to a local charity. Are we able to donate the equipment after sanitizing the hard drive?
4. When should storage media be degaussed?
5. Who do I contact for degaussing storage media?
6. Who do I contact with additional questions about the policy and/or further assistance?

Answers:

1. Yes. All systems must be sanitized when transferred from one employee to another, even if the two employees perform similar functions.
2. Contact your Information Technology personnel for assistance sanitizing storage media.
3. No. Any hardware that is donated or discarded must not include any memory (i.e. RAM) or storage media such as hard drives, USBs, printers, backups tapes, etc.
4. Storage media must be degaussed at the end of a system's life cycle at the University, if the system will be donated or thrown away.
5. Contact central IT Security to schedule a pickup of your equipment by emailing security@miami.edu.
6. For questions about the policy and/or additional assistance contact the Chief Information Security Office at ciso@miami.edu.

➤ IT Audit Policy (A125)

No audit related work or inquiries will be conducted without VP approval and having informed the appropriate departmental leadership, but if you have any questions and/or concerns regarding any current or planned audit initiatives contact the Chief Information Security Office at ciso@miami.edu.

➤ IT Security Incident Response Notification (A160)

Questions:

1. What is Incident Response Notification?
2. What are security incidents?
3. What are common examples of security incidents?
4. To whom should I report a security incident?

Answers:

1. The process created and communicated to constituents empowering them to identify and report any suspicious events which may be security incidents.
2. A security incident is any event or series of events that impact the security or ability of the University to continue normal educational and business operations.
3. Examples of security incidents include:

- a. Email with suspicious content from known or unknown sender(s)
 - b. Files missing and /or corrupted
 - c. Equipment and media is lost or stolen (Laptop, thumb drive, CD, etc)
 - d. Sensitive data is sent to non-authorized user(s)
 - e. A hardcopy report is lost or stolen containing sensitive information
4. Any suspected and/or confirmed security incident should be report to your immediate supervisor. Individuals in supervisory roles should escalate reports of security incidents through their appropriate communications channel.

➤ IT Security Incident Response Procedures (A165)

Questions:

1. What are Incident Response Procedures?
2. What are security incidents?
3. Who do I get started building incident response procedures in my areas?
4. Who do I contact with additional questions about the policy and/or further assistance?

Answers:

1. A plan designed to detect report, mitigate, and remediate any security incidents that may arise with the potential to have negative consequences to the University. The goals of the procedures include:
 - a. Maintaining and restoring business continuity
 - b. Defending against future attacks
 - c. Deterring attackers through investigation and prosecution
 - d. Performing counter-intelligence/intelligence activities where appropriate
2. A security incident is any event or series of events that impact the security or ability of the University to continue normal educational and business operations.
3. The following supplemental materials are intended to assist an IT organization document and establish appropriate incident response procedures ([Click here to access the supplemental documents](#)).
4. For questions about the policy and/or additional assistance contact the Chief Information Security Office at ciso@miami.edu.

➤ Remote Access (A190) (emailed Jose for info on SSL VPN)

Questions:

1. Does the University offer any solution for remotely accessing University resources and data securely?
2. How do I obtain access to the SSL VPN?
3. Who do I contact with technical issues related to the SSL VPN (sphinx.miami.edu or www.miami.edu/vpn)?
4. Who do I contact for with additional questions about the policy and/or for further assistance?

Answers:

1. Yes, the University offers an SSL VPN solution that is accessible via the following URL: <http://sphinx.miami.edu> or www.miami.edu/vpn .
2. Every employee, faculty, staff, etc. with a CaneID is able to log into the SSL VPN without having to initiate a formal request for access. To access the SSL VPN simply open a web browser and type sphinx.miami.edu.
3. For technical issues related to the SSL VPN (sphinx.miami.edu or www.miami.edu/vpn) contact central IT security by emailing security@miami.edu.

4. For questions about the policy and/or additional assistance contact the Chief Information Security Office at ciso@miami.edu.

➤ Access Control User Account Management (A130)

Questions:

1. How do I get access to central systems?
2. I have an application and need to authenticate and/or authorize users. What are the options for authentication and authorization?
3. What is an employee's internal unique identifier?
4. What if my application does not meet the requirements for this policy?
5. When creating user accounts for individual applications, may I create accounts to mirror a user's CaneID?

Answers:

1. Information Technology uses two primary methods to grant access, Cane ID and IDMS. A CaneID account is required to access the majority of central applications including UMail, myUM, Blackboard and UMeNET (Ariba) . You can create a CaneID online at <https://caneid.miami.edu/createnewaccount.aspx>. An IDMS account is required to access administrative applications such as the HR, Student and Financial systems, DMAS and UMAPPS. An IDMS account can be request by completing the online request form at http://www7.miami.edu/um_global_static_files/itsecurity_department_files/idmsaccess.htm.
2. For web-based applications, CaneID Authentication Service (CAS) is an option that provides authentication and high-level authorization information. It uses Cane ID to validate the user and if successfully validated provides biographical and organizational information about the user to the application that the user is accessing. This allows that application to create accounts on the fly and/or update user profiles with the most up to date information. For more information on CAS, download the Cane ID Authentication Service (CAS) Introduction guide. For applications that are not web-based, we would suggest using the LDAP authentication against the Central Directory. For more information, please contact security@miami.edu .
3. The employee's internal unique identifier is the UMID (i.e. – C00000000). The UMID (or SSN for that matter) should not be used as the login username for any system. The UMID should be used for internal searching, matching, indexing and processing on the backend system only.
4. Refer to the exceptions section of the policy for appropriate action. If you have questions after referring to the exception section please contact security@miami.edu.
5. Application accounts should not mirror a user's CaneID.

➤ Encryption (A175)

Questions:

1. How does email encryption work?
2. Does the University have software for disk encryption?
3. How can I get my desktop or laptop computer encrypted?
4. Will encryption affect my ability to use my computer?
5. Can any USB device be encrypted or do I need a specific one?
6. What is FTP?
7. I am a system administrator and need to send and receive FTP. Does IT provide a secure FTP solution?
8. Someone requested that a file be sent to them FTP. How do I FTP securely?
9. What is the recommended method to encrypt a file I want to send via email?

10. What is the recommended method to encrypt a file I want to place on a shared drive or FTP to another party?

Answers:

1. Details on email encryption can be found at <http://www.miami.edu/securemail>. This page contains an overview of email encryption works, what data should be encrypted and instructions on sending a secure email.
2. The University uses Pointsec which is whole-disk encryption software for portable and desktop computers.
3. Please contact security@miami.edu for more information.
4. No, once the software is installed you will be able to use your computer just as you normally would.
5. Any device can be encrypted. However, the encryption method/standard of the encryption software used to encrypt the device is important. Currently, IT recommends the following standards: 3DES, Blowfish, RSA, RC5 or IDEA.
6. FTP stands for File Transfer Protocol and is a method widely used for transferring files between two systems within an organization or across the Internet. This protocol has no security and as a result any login and password information is sent in plain text.
7. Please contact security@miami.edu for more information.
8. If the file is encrypted already, then you can send it via standard FTP. You should provide the encryption key to the other party via alternate means (i.e. - Don't include it in the FTP transmission as the user id or password or as a separate FTP to the same location!)

You should be very cautious when sending data outside of the University! You should be certain of the identity of the individual and/or company you are sending it to, that the contracts and/or support agreements with that company are in proper order to release data to their care and that all compliance issues are satisfied. If you have any questions or concerns about sending data outside the university, please contact security@miami.edu for assistance.

9. Email encryption will handle encrypting the body of the email and all file attachments. Put "[secure]" somewhere in the subject line, without the quotes to ensure that the email is encrypted. Details on email encryption can be found at <http://www.miami.edu/securemail>. This page contains an overview of email encryption works, what data should be encrypted and instructions on sending a secure email.
10. Please contact IT security for consultation and assistance at security@miami.edu.

➤ Malicious Software Prevention Policy (A170)

Questions:

1. Where can I get anti-virus / anti-malware protection software?
2. What if my application vendor prohibits the installation of such software?

Answers:

1. Symantec Endpoint Protection detects and eliminates destructive pests like trojans, spyware, adware and hacker tools. This software is provided free of charge to all enrolled students and faculty/staff of the University of Miami. Symantec Endpoint Protection can be download from <http://www.miami.edu/software> (could link directly to AV http://www6.miami.edu/UMH/CDA/UMH_Main/1,1770,31349-1;31949-2;37253-3,00.html).
2. Refer to the exceptions section of the policy for appropriate action. If you have questions after referring to the exception section please contact security@miami.edu.

➤ Mobile Computing (A180)

Questions:

1. How to establish a PIN on my mobile devices?

Answers:

1. List method to establish pin/password on common devices
<content to follow>

➤ Password Security (A131)

Questions:

1. What are the characteristics of a strong password?
2. Is it ever acceptable to share my password?
3. I am a system administrator and have a process / job / service that requires a domain level service account. How can I request this account?
4. I am a system administrator and have an application that can use domain level groups. How can I request a group be created?

Answers:

1. Passwords must be at least 7 characters and consist of at least three of the following three character types: upper and lower case alpha characters, numeric characters, and symbols.
Additionally, you should change your password immediately upon:
 - Learning a password has been compromised;
 - A security breach is suspected;
 - Learning a password has been shared with another individual;
 - Changes of personnel or personnel leaving University (i.e. departmental inbox); or,
 - User no longer requires access to the system.
2. No! You should never share your password. Not with your colleagues, supervisor or even IT Security! There is no reason for anyone besides you to know your password.

We often hear “I need to respond to email on behalf of my supervisor” or “I need to submit grades on behalf of our department’s faculty”. Information Technology has methods to grant proxy access to facilitate these or similar circumstances. If you need assistance with such an issue, please contact the IT Support center at 305-284-6565 for assistance.

3. Contact IT Security for assistance by sending an email to security@miami.edu.
4. Contact IT Security for assistance by sending an email to security@miami.edu.