**Contingency planning**

**Policies and their weaknesses**

CP0001:

|  |  |
| --- | --- |
| [Maintaining Information Security During a Disaster](http://security.ufl.edu/wp-content/uploads/2013/09/CP0001.pdf) How to treat information assets and systems in the case of an emergency or other event which compromises or damages systems. | 02/22/2010 |
|  |  |

1. Specifies how to treat information in case of any disaster

**Policy:**

* In case of disaster
  + Preparation for an impending event
  + Immediate aftermath of the event
  + Implementation of contingency plans
  + Recovery and return to normal operation
* Procedures should be written to continue business after a disaster and to protect all classified and restricted information
  + There should be copies of these procedures in an offsite location
  + The required software and systems that are to be used for continuation of business should be documented and the procedures such as how to recover the data should be written.
* Data theft is considered a security incident, if the data theft occurs, then the data integrity and validity should be checked before using the data

**Weaknesses and things to improve:**

* In data breaches, a crisis management should be present, to go in depth and check anything else other than the known information is revealed, such as if data theft occurred, verify if any other data or possible defense mechanisms are breached and integrity of required data should be checked based on how crucial the information is
* Not all the data can be restored during the peak times, but it should be made crucial to prioritize the information that is very essential to the business and appropriate actions should be taken to the recover the most out of this crucial data.

|  |  |  |
| --- | --- | --- |
| CP0002 | [Contingency Plan](http://security.ufl.edu/wp-content/uploads/2013/09/CP0002.pdf) Requirements for a plan departments must make ready in case of a disaster event as described in CP0001. | 02/22/2010 |

Policy:

* Each unit need to have a written contingency plan
  + They can use the CP0002.4 as a standard to write the contingency plan
  + It will be the responsibility of the Unit Information Security administrator (ISA) to verify if the requirements to perform the contingency plan are set in place.
* If CP0002.4 is not used, then it should be verified to check if proper requirements are met.
* The main problems to be taken care by the contingency plan are:
  + Restore critical business process per policy CP0001
  + Recover the classified assets as per policy CP0002.02
  + Prepare for possible disasters such as data theft, natural disasters etc.
* Responsibility:
  + The unit ISA has to verify if all requirements are set for the contingency plan and they comply with the contingency planning policies
  + The unit information security manager should be in charge of the Unit ISA to verify if the Unit ISA is perform the planning properly. If not he should inform the Dean, the director or the department chair in writing.
  + The contingency plan will contain writing about which person is responsible for a particular unit to perform the contingency plan. This will be the unit contingency plan coordinator
* Plan review:
  + The plan should be reviewed annually
  + The plan needs to updated based on deficiencies observed
* Documentation
  + The offsite copies of the updated plans should be maintained by
  + Unit ISA
  + Unit ISM
  + Senior person in the unit such as dean or department chair or the director
  + The Health science center HSC chief
  + Contingency plan coordinators and their backups
  + Annual process
    - Unit ISA should review the procedures
    - Unit ISM or other senior person should should check and approve the plan with date and signature
    - The updated plan should be sent to HSC chief and he will maintain the plans for both offsite and onsite
* Training:
  + The Unit ISA should conduct annual tests for each new procedure that is added to the plan.
  + Recovery teams should be trained to perform the recovery and their independent roles in such event
  + Document and record the personnel who has undergone the training
* Testing
  + Written procedures should be placed to perform the disaster recovery plan for testing once a year or as required. This should be taken care by the contingency plan coordinator
  + It is good to practice individual procedures at a time so as not to affect the business as a whole
* Reporting:
  + Annual reporting of the disaster recovery testing success and failures of both planning and implementation should be well documented and forwarded to HSC chief
  + The HSC chief will be responsible to note
    - Units who have not completed annual training or reporting
    - Testing for new procedures done by units and exceptions
    - Updating of procedures or reviews annually by the unit
  + The senior VP of health affairs shall will initial the summary report and hand over again to HSC chief. The people who have not followed the policy shall be subject to sanctions policy Policy GP0002

**Weaknesses and things to improve:**

* Each unit is responsible for their team. It would improve the procedures In contingency planning if someone outside the unit reviews the plan to get a thorough insight in to the planning.
* There should be multiple contingency plans incase both onshore and offshore site is compromised such as an offline backup facility.
* Backup should always be available in case one of the unit is unavailable to continue the procedure.
* During testing using simulations for the disaster and then trying it on a virtual simulator would be a good idea, since all the plans cannot be testing onsite.
* Detailed steps should be written in an order so that there won’t be overlap of plans and recovery in between.
* During the testing phase, the time duration should b noted to analyze how long it will take to recover in case of a disaster so as to have a time set to tell the clients about the recovery period.
* The clients, stake holders, employees and customers should be made known of the disaster recovery plan as required.
* The recovery teams should be well trained in both virtual and onsite scenarios to recover the information based on priority to get the business running.
* Strategies should be planned based on the existing disasters that have occurred and plans to recover from such disasters. This should be made well known to the personnel handling the disaster recovery plan and recovery.
* There should be plans to check the after math in detail, such as validate the things that are successful and that have failed to be recovered and contingencies for the failed processes and their impact on the organizations.
* Documentations should be done while performing the disaster recovery plan, such as
* who is executing the plan
* the stages being followed
* If they are complained with the planned policy
* The personnel involved in the planning
* To check if proper milestones have been reached as planned, if not alternate ways to lessen the damage and proceed the business.

|  |  |  |
| --- | --- | --- |
| CP0002.02 | [Risk Assessment – Mission Crucial Systems](http://security.ufl.edu/wp-content/uploads/2013/09/CP0002-02.pdf)  [Relative Criticality Approach](https://security.ufl.edu/policies/healthcare-information-security-policies/contingency-planning/) [HSC Crucial Info Systems Registry Worksheet](https://security.ufl.edu/policies/healthcare-information-security-policies/contingency-planning/) | 02/22/2010 |

* The unit ISA is responsible for performing IT risk assessment to be conducted bi annually to identify the value of information and assets, replacement costs, acceptable data loss and downtimes.
* Procedures in the units contingency plan should be based on the risk assessment
  + All crucial assets should be in the contingency plan
  + Plan to address disaster preparation, recovery, aftermath, long term recovery and restoration etc. should be well written and detailed.
  + Use of offsite locations, alternative locations and equipment’s should be included
  + For information, not under crucial, there should be procedures to restore availability
  + The reassessment can be used to classify the information and assets into crucial and non-crucial
* Documentation should be done to all the crucial assets and information

**Weaknesses and things to improve:**

* Risk assessment should also include how the clients will be impacted due to the disaster and how their data is being backed up and restored.

|  |  |  |
| --- | --- | --- |
| CP0002.04 | [Contingency Planning Template](https://security.ufl.edu/wp-content/uploads/2013/09/CP0002-04.pdf) | 02/22/2010 |

Contingency planning template:

* Record of Changes

• Individual Record of Receipt of Contingency Plan

• Annual Review of Contingency Plan by the Information Security Administrator

• Annual Approval of Contingency Plan by the Dean, Director or Department Chair

• Activation Authority

• Unit Points of Contact

• Emergency Points of Contact Outside of the Unit

• Identification of Information Assets and Risk Assessment

• Emergency Protection Plan for Physical Media Containing Restricted Information

• Emergency Protection Plan for Restricted Information Stored as Accessible Data

• Mapping of Applications and Systems to Restricted Data Security

• Identification of Crucial Assets and Dependencies; Development of Contingency Plans

• Preparation Checklists

• Data Backup Procedures and Offsite Storage Locations.

• Data Restoration Procedures.

• Record of Testing Procedures for Restoration from Backup

• Record of Training

• Record of Testing Contingency Plan

• Mission Crucial System History

**Weaknesses and things to improve:**

* Backups to the point of contact
* Backup for approval in case of a higher official is not available to approve the procedure during disaster
* Records of personnel involved in the planning, testing and implementation phases.
* Risk assessment of each asset and information
* Point of contact and their backup information to be made know to personnel to notify about the diaster