BUSINESS CONTINUITY

SOURCE: Ohio IT Policy; ITP-B1 Ohio IT Policy; ITP-E7

CONTACT: INFORMATION TECHNOLOGY SERVICES

Purpose

This policy is to provide Ohio EPA with information to guide the development of business continuity plans and procedures for computer and communications services.

Background

The need for business continuity planning and operations pertaining to the services offered by Ohio EPA is becoming more critical as more services are offered via computer and data network technologies. As a result, it is essential that Ohio EPA define availability objectives for each offered service and define business continuity plans and related procedures that will achieve the desired service availability. Services that must be available during specific time intervals or possibly at all times must have an appropriate operational architecture so that natural events (i.e. hardware or power failure) can be resolved quickly. If an event occurs that renders the service location unusable (bomb, earthquake, bio-terrorism), it may be necessary to have an alternate location sufficiently far away from the primary location to not be affected. It may even be necessary to assign alternate personnel to perform functional roles.

Business Continuity is not limited to information systems disaster recovery. Business Continuity is a holistic and multi-disciplinary process that is proactive to define, implement, and test the plans and procedures needed to insure that business services can continue to be offered when any failure event occurs. Failure events can be due to natural events, accidental events, and malicious events. Events can cause limited, focused damage or elimination of all service related resources. As a result, good business continuity planning includes a layered set of procedures that can effectively deal with recovery of one or more of the following resources:

1. Personnel
2. Computer and Networking Equipment
3. Infrastructure Utilities (e.g. Commercial Power, Telephone, ISP, Water, etc.)
4. Building space and environmental controls
5. Office supplies including forms and miscellaneous office equipment

6. Documentation:

    a. Emergency response contact lists

    b. Operational Processes and Procedures

    c. Business Continuity plans and procedures

Business interruptions can result in loss of reputation, loss of business to competitors, human resource issues, health and safety issues, collateral damage to customers, and higher insurance premiums. A serious business interruption could even lead to business failure.

In developing a business continuity strategy and plan, Ohio EPA planners must consider the cost to implement backup and recovery plans and reach an appropriate balance with the impacts from a service outage.

Business Continuity Policy

Ohio EPA's services are supported by a variety of platforms. For example, mainframe logical participations provide the platform for services provided to some Agencies. Linux servers and Windows servers provide the platforms for services to other Agencies. Complex data networks support communications. These platforms and their associated networking facilities should be sufficiently diverse to achieve the availability needed by the application service offerings. As a result, this policy provides the foundation considerations for business continuity that are needed to define individual platform and application back-up and recovery procedures plus other procedures applicable to a disaster declaration.

1. General

a. Ohio EPA must have business continuity plans to insure reliable delivery of services. The Plan shall be tested and updated at least annually, but preferably every six months, to assure its validity. This includes testing recovery from localized failures and recovery from disaster events.

b. Business continuity plans should be designed to reduce the consequences of any loss of services to an acceptable level. They are not just planned responses to major catastrophes. The purpose of a business continuity plan is to mitigate the damaging consequences of unexpected and undesirable events of whatever magnitude (i.e. hardware or software failures, power outages, environmental control failure, etc). While it is true that data processing personnel must plan for catastrophic loss, it is also true that they must plan for less-than-catastrophic events (e.g. localized hardware failures, software corruptions, and data

corruptions) that also cause an interruption of Ohio EPA supported services.

c. Ohio EPA shall establish availability requirements for each supported service. Availability requirements must be known before proper service architectures, maintenance strategies, and back-up/recovery strategies can be defined. Some services may be designated as mission critical. Others may tolerate an extended service outage with minimal consequences.

d. OHIO EPA shall inventory hardware and software components supporting each service. The following information should be recorded:

Software:

1) Name and version number
2) Software keys
3) Vendor name and address
4) Vendor telephone, pager, and FAX numbers
5) Date of purchase
6) Maintenance contract reference number and expiration date

Hardware:

7) Hardware model and serial number
8) Vendor name and address
9) Vendor telephone, pager, and FAX numbers
10) Date of purchase
11) Maintenance contract reference number and expiration date

e. When planning new services or upgrading existing ones, OHIO EPA shall define service architectures that are capable of meeting service availability requirements.

f. Hardware and software maintenance procedures shall be capable of recovering from hardware component failures or software anomalies within allotted downtime intervals.

g. Special arrangements should be made for hardware and software that has been declared obsolete by a vendor and is no longer supported by the vendor or where the vendor is no longer in business. Special arrangements can include special one-time buys of hardware field replaceable units or special vendor support contracts.

h. In the event of commercial power failures, OHIO EPA shall provide uninterruptible power supplies (UPS) to maintain IT resources for 30 minutes.

i. Environmental control facilities shall be implemented with redundancy or have repair parts availability sufficient to recover from environmental control failures within the allotted downtime interval.

j. Software and data back-up scope and frequency shall be aligned with acceptable loss of data. Back-up media shall be retrieved and service restored within the allotted downtime interval. Back-ups shall be stored in an off-site secure facility.

k. Staffing plans shall have sufficient redundancy such that vacations, illness, and accidents do not compromise service availability.

2. Localized Failure Events

a. Response to localized failures (e.g. Hardware component failures, software and data corruptions) should be covered by normal OHIO EPA operational procedures that are defined to meet service availability objectives.

b. OHIO EPA shall establish a hardware repair procedures that meet allocated downtime objectives. Replacement of hardware field replaceable units may require availability of on-site spares if the downtime allocation for this type of failure is less than four hours. If longer downtimes are permissible, vendor response and repair may be sufficient and must be specifically agreed to by the vendor.

c. OHIO EPA shall define software restoration procedures that meet allocated downtime objectives. Software restoration may be achieved by a restart or may require a reload from backup media or vendor supplied media.

d. OHIO EPA shall define data restoration procedures that meet allocated downtime objectives. Data restoration typically requires a data reload from backup media followed by user updates to recover data that was entered after the backup media was created and before the failure event occurred. In rare occasions, it may be possible to repair the operational data set.

e. OHIO EPA shall define procedures to recover environmental controls so that IT equipment does not exceed minimum and maximum temperature and humidity limits. These procedures can include timely repair of environmental controls, environmental control redundancy, and powering down of unessential equipment.

3. Disaster Declaration

The scope and impact from a disaster event is far greater than failures caused by localized events. As a result, the scope of disaster recovery plans and procedures is also far greater, more complicated and expensive to implement. Disaster events may include fire, flood, earthquake, tornados, hurricanes, civil disorder, bombs, chemical, biological, and radiological attacks.

The software and data backup procedures implemented to support localized failures should also be sufficient to support a disaster recovery event. Having a different set of procedures would only complicate OHIO EPA operations.

Other considerations are unique to a disaster event and need to be recognized and documented in the disaster recovery plan.

a. Triggers for declaring a disaster shall be defined. A disaster declaration typically involves the replacement of major resources required to provide a mission critical service. An alternate site, alternate IT systems, and alternate personnel may be required.

b. The disaster recovery site shall be located far enough from the primary site so that one event does not affect both. Location should consider the utility infrastructure to insure that both the primary and recovery sites are not served by the same commercial power, telephone, ISP, water, and sewer facilities.

c. Based upon the results of a risk analysis, OHIO EPA shall define which services are mission critical and what resources require an alternate site capability to recover the service should the IT resources at the primary site be rendered unusable. It may be permissible for some services to remain down until the primary site is rebuilt or restored.

d. The Computer Incident Response Team (CIRT) shall be defined and documented in order to establish command and control in a disaster event. Roles shall be clearly defined. A member of the

emergency response team shall be identified to serve as liaison to other state and federal emergency response teams.

e. Procedures needed to operate mission critical services, including back-up and recovery procedures shall be documented.

f. If software licensing forbids copying of software, support agreements must be obtained to insure that the vendor will provide replacement copies or authorize the copying and restoration of existing software within the desired recovery interval.

g. The following items shall be stored at a secure off-site location:

- A copy of the disaster recovery plan and associated procedures
- A copy of the CIRT list
- Back-up media containing platform software, application software, and data
- A copy of the procedures needed to operate mission critical services, including back-up and recovery procedures
- A copy of vendor's operations and maintenance documentation
- Any office supplies not readily available from commercial sources
- A copy of up-to-date software and hardware inventories

h. Disaster recovery plans and procedures shall be tested at minimum annually, but recommended every 6 months or when significant revisions to the service architectures are implemented.

4. Disaster Recover Plan Structure and Contents

The OHIO EPA disaster recovery plan should follow the outline recommended in Ohio IT Policy; ITP-E7; Business Resumption Planning. A summary of this outline follows.

a. Planning
    1) Purpose
    2) Scope
    3) Assumptions
    4) Responsibilities
    5) Strategy

i. Emergency Response
ii. Backup Operations
iii. Recovery Actions

6) Record of Changes
7) Plan Security

b. Preparatory Actions
1) People
2) Data
3) Software
4) Hardware
5) Communications
6) Supplies
7) Transportation
8) Space
9) Power and Environmental Controls
10) Documentation

c. Action Plan
1) Emergency Response
2) Backup Operations
3) Recovery Actions

d. Testing

Compliance

Any employee found to have knowingly violated this policy may be subject to disciplinary action, up to and including termination of employment

Definitions

None

NOTE: This policy is one of many Ohio EPA Security Policies. Ohio EPA Security Policies should be considered collectively rather than as separate or unrelated. For example Security Incident Response is an important companion to this policy.

Direct inquiries about this policy to:

Office of Information Technology Services
Ohio Environmental Protection Agency
50 West Town Street, Suite 700
P.O. Box 1049
Columbus, Ohio 43216-1049
Telephone: 614-644-3010
Email: Skip.Holler@epa.state.oh.us

10/08