



STATE OF WASHINGTON
DEPARTMENT OF CORRECTIONS

APPLICABILITY
DEPARTMENT WIDE

REVISION DATE
1/21/16

PAGE NUMBER
1 of 3

NUMBER
DOC 280.300

POLICY

TITLE
**INFORMATION TECHNOLOGY (IT) DISASTER
RECOVERY**

REVIEW/REVISION HISTORY:

- Effective: 4/15/95
- Revised: 6/1/05
- Revised: 9/6/07
- Revised: 11/21/08
- Revised: 9/7/09
- Revised: 9/12/11
- Revised: 11/12/12
- Revised: 1/21/16
- Reviewed: 2/17/20

SUMMARY OF REVISION/REVIEW:

Reviewed only. No changes made.


APPROVED:

Signature on file

STEPHEN SINCLAIR, Secretary
Department of Corrections

2/10/20

Date Signed

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/21/16	PAGE NUMBER 2 of 3	NUMBER DOC 280.300
	TITLE INFORMATION TECHNOLOGY (IT) DISASTER RECOVERY		

REFERENCES:


DOC 100.100 is hereby incorporated into this policy; [OCIO 151 Information Technology Disaster Recovery Planning](#)

POLICY:

- I. The Department has developed and maintains Information Technology (IT) disaster recovery/business continuity plans to ensure the continuation of critical IT dependent services during recovery from a business disruption, including a major disaster.

DIRECTIVE:

- I. General Responsibilities
 - A. The Chief Information Officer will ensure the maintenance of an IT disaster recovery plan which will allow the recovery of mission critical computing and telecommunications services after a business disruption.
 - B. The IT disaster recovery/business continuity plan coordinator will notify IT employees/contract staff of the plan and how to execute it.
 - C. The Chief Information Security Officer/designee will audit the IT disaster recovery plan for compliance with Department and Office of the Chief Information Officer (OCIO) policies and standards.
 - D. The Secretary will include a letter in the IT portfolio indicating the degree of compliance with OCIO disaster recovery/business continuity policies.
- II. IT Disaster Recovery/Business Continuity Plans
 - A. IT disaster recovery/business continuity plans will identify:
 1. All critical IT dependent operations and the priority sequence for restoring these services.
 2. Significant threats and methods to mitigate risk.
 3. The maximum amount of data loss the Department can sustain for each critical IT dependent operation.
 4. The maximum amount of time the Department can tolerate the loss of IT services for each critical IT dependent operation.
 5. IT employees responsible for:

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/21/16	PAGE NUMBER 3 of 3	NUMBER DOC 280.300
	TITLE INFORMATION TECHNOLOGY (IT) DISASTER RECOVERY		

- a. Declaring the level of disaster, and
- b. Implementing the plan.

III. Updating/Maintenance

- A. The IT disaster recovery/business continuity plans will be reviewed and updated annually or whenever there are significant changes to the Department computing environment to ensure compliance with the OCIO disaster recovery/business continuity policies and standards.

IV. Testing

- A. IT will test the IT disaster recovery plan process annually and document findings to ensure its integrity and compliance with OCIO requirements.

V. Training

- A. IT employees will be trained to execute the disaster recovery plan to include:
 1. Ensuring employees are aware of the need for a disaster recovery/business resumption plan.
 2. Being aware of their responsibilities and what procedures to follow during the disaster discovery process.
 3. Practice for the recovery team of disaster recovery/business resumption skills.

DEFINITIONS:

Words/terms appearing in this policy may be defined in the glossary section of the Policy Manual.

ATTACHMENTS:

None

DOC FORMS:

None