STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **DEPARTMENT WIDE**		
	REVISION DATE 3/18/25	PAGE NUMBER 1 of 3	NUMBER **DOC 280.300**
POLICY	TITLE **INFORMATION TECHNOLOGY 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
Revised:	1/11/21
Revised:	3/18/25

SUMMARY OF REVISION/REVIEW:

Updated terminology throughout
I.C., I.D., and II.B. - Adjusted language for clarification
II.A.4. and II.A.5. - Added clarifying language
Added II.B.1. that test objectives, results, and corrective actions/risk mitigations will be documented, and plans will be updated as needed
Removed II.C. that IT will test the IT disaster recovery plan process annually

APPROVED:

Signature on file

TIM LANG, Secretary
Department of Corrections

2/14/25
Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; Information Technology Disaster Recovery Planning

POLICY:

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

DIRECTIVE:

I. 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/COOP 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 Washington Technology Solutions (WaTech) policies and standards.

D. The Secretary/designee will include a letter in the IT portfolio indicating the degree of compliance with WaTech disaster recovery/COOPs.

II. IT Disaster Recovery/COOPs

A. IT disaster recovery/COOP plans will identify:

1. All critical IT dependent operations and the priority sequence for restoring these services.

2. All critical dependencies on systems, components, or service providers not directly under Department control.

3. Significant threats and methods to mitigate risk.

4. The maximum amount of data loss the Department can sustain for each critical IT dependent operation (i.e., recovery point objective).

5. The maximum amount of time the Department can tolerate the loss of IT services for each critical IT dependent operation (i.e., recovery time objective).

6. IT employees responsible for:

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

B. IT disaster recovery/COOP plans will be reviewed, updated, and tested at least every other year or within 90 days of the production date when there are significant changes/upgrades or new applications.

   1. Test objectives, results, and corrective actions/risk mitigations will be documented and plans will be updated as needed.

III. Training

A. Designated 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