
	<b>PINAL COUNTY</b> Business Continuity and Disaster Recovery		
	DATE: 08/26/2020 REVISED:	PAGES: 7	POLICY NUMBER: 11.005

## Business Continuity and Disaster Recovery Standard

### Table of contents

<b>PURPOSE</b>	<b>2</b>
<b>AUTHORITY</b>	<b>2</b>
<b>SCOPE</b>	<b>2</b>
<b>RESPONSIBILITY</b>	<b>2</b>
<b>COMPLIANCE</b>	<b>3</b>
<b>STANDARD STATEMENTS</b>	<b>3</b>
<b>Business Continuity Management</b>	<b>3</b>
<b>Disaster Recovery Management</b>	<b>5</b>
<b>CONTROL MAPPING</b>	<b>7</b>
<b>RELATED DOCUMENTS</b>	<b>7</b>
<b>DOCUMENT CHANGE CONTROL</b>	<b>7</b>

	<b>PINAL COUNTY</b> Business Continuity and Disaster Recovery		
	DATE: 08/26/2020 REVISED:	PAGES: 7	POLICY NUMBER: 11.005

## 1. PURPOSE

- 1.1 Business Continuity and Disaster Recovery – The purpose of this standard is to establish procedures for the continuation of critical business processes in the event of any organizational or Information Technology (IT) infrastructure failure, and define the related controls and acceptable practices. Pinal County has roles in different areas of Critical Infrastructure Sectors; Healthcare and Public Health, Emergency Services, Financial, Transportation and Government Facilities. As a government entity we strive to keep these sectors and their services functioning.

## 2. AUTHORITY


- 2.1. Pinal County provides that “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all departments shall adhere to the policies, procedures and objectives established by the Information Security Department with respect to activities concerning information technology.”

## 3. SCOPE

- 3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of Pinal County. The document applies to all county departments including all boards, commissions, divisions, councils, bureaus, and offices. Other County entities that voluntarily use or participate in services provided by the Information Technology Department, such as PinalCountyAZ.gov, must agree to comply with this document, with respect to those services, as a condition of use.

## 4. RESPONSIBILITY

- 4.1. The Information Security Department is responsible for the development and ongoing maintenance of this standard.
- 4.2. The Information Security Department is responsible for compliance with this standard and may enlist other departments in the maintaining and monitoring compliance with this standard.
- 4.3. Any inquiries or comments regarding this standard shall be submitted to the Information Security Department by sending an email to [ITSecurity@Pinal.gov](mailto:ITSecurity@Pinal.gov).

	<b>PINAL COUNTY</b> Business Continuity and Disaster Recovery		
	DATE: 08/26/2020 REVISED:	PAGES: 7	POLICY NUMBER: 11.005

4.4. Additional information regarding this standard may be found at <https://www.pinalcountyz.gov/HR/Pages/PoliciesProceduresRules.aspx>.

## 5. COMPLIANCE

5.1. Compliance with this document is mandatory for all departments including all executive offices, boards, commissions, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the County. Exceptions to any part of this document must be requested via email to the Security Department ([ITSecurity@Pinal.gov](mailto:ITSecurity@Pinal.gov)). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Pinal County Chief Information Security Officer (CISO) or appointed designee.

## 6. STANDARD STATEMENTS

### 6.1. Business Continuity Management

All Departments must establish a Business Continuity Program.


6.1.1. All Departments must develop and maintain processes for business continuity, as follows:

6.1.1.1. Identify a Business Continuity Lead that will have primary responsibilities for the Business Continuity Program, including plan development, plan testing and program sustainment.

6.1.1.2. Perform a risk assessment of critical information assets: Establish controls to identify, contain and mitigate the risks associated with the loss or disruption of critical business processes and information assets (see *Information Security Risk Management Standard 11.010* for additional detail on risk assessments).

6.1.1.3. Conduct Business Impact Analysis (BIA): Each department must leverage the *Asset Management Standard 11.004* when applicable, to perform a BIA to identify critical business processes, information assets, customers, third parties, technical and non-technical dependencies, and recovery timelines and to assess the impact a disruption would have on the organizational processes, systems and operations.

6.1.1.3.1. The BIA shall be updated whenever a major organizational change occurs or at least annually, whichever comes first.

	<b>PINAL COUNTY</b> <b>Business Continuity and Disaster Recovery</b>		
	DATE: 08/26/2020 REVISIED:	PAGES: 7	POLICY NUMBER: 11.005

6.1.1.4. Develop Business Continuity Plans (BCP): Each department shall develop BCP's for critical business processes based on prioritization of likely disruptive events in light of their probability, severity and consequences for information security identified through the BIA and risk assessment processes.

6.1.1.4.1. BCP's shall address both manual and automated processes used by the department and document minimum operating requirements to resume critical functions/applications in an appropriate period of time.

6.1.1.4.2. The primary responsibility for developing, maintaining and testing organizational and functional BCP's shall reside with the Business Continuity Lead.

6.1.1.4.2.1. Roles and responsibilities of BCP stakeholders shall be clearly defined, communicated and agreed upon.

6.1.1.4.2.2. Point(s) of contact should be identified from the customer side for any incident or crisis communication via call, messaging and/or email. The contact details of the point(s) of contact should be validated and updated at least annually.

6.1.1.4.3. BCP's shall be updated whenever a major organizational change occurs or at least annually, whichever comes first.

6.1.1.4.4. BCP's shall be developed as follows:


6.1.1.4.4.1. Create and implement adequate business recovery and risk mitigation strategies, including the definition of acceptable recovery time frames.

6.1.1.4.4.2. Clearly state the condition(s) required for activating BCP's to minimize the cost associated with unnecessary use.

6.1.1.4.4.3. Define fallback and resumption emergency procedures to allow for temporary measures and full resumption as required. Ensure that confidential information is protected while operating in emergency mode.

6.1.1.4.4.4. Assess BCP impact to external organizational dependencies and contracts.

6.1.1.4.4.5. Develop public relations strategy to ensure effective and timely communication to relevant stakeholders.

	<b>PINAL COUNTY</b> Business Continuity and Disaster Recovery		
	DATE: 08/26/2020	PAGES: 7	POLICY NUMBER: 11.005

6.1.1.4.5. Business Continuity Lead shall schedule and evaluate BCP testing procedures to ensure that they are practical and realistic.

6.1.1.4.5.1. Perform annual tests of the BCP's to identify incorrect assumptions, oversights and account for updates to equipment or personnel changes. Test results shall be reported to senior management and the Information Security Department.

6.1.1.4.5.2. All relevant stakeholders associated with BCP procedures shall participate in annual testing. A debrief session to evaluate test results and to discuss lessons learned should be conducted following the test.

6.1.1.4.5.3. If significant changes are implemented to BCP's, testing cadence must be reevaluated and executed.

6.1.2. **Information Owner** shall develop backup standard operating procedures that are in alignment with the *Operations Management Standard 11.012* and specifically *Data Backup and Restoration in the Operations Management Standard 11.012* to ensure that copies of critical data are retrievable.

## 6.2. Disaster Recovery Management

All Departments must ensure that Disaster Recovery (DR) procedures shall be initiated when the appropriate personnel has determined the ability to recover critical information assets will likely exceed the established recovery time and/or recovery point objectives. Adequate backup facilities should be provided so all essential information assets can be recovered following a disaster.


6.2.1. All Departments must develop and maintain processes for disaster recovery plans at both onsite primary County locations and at alternate offsite locations. DR plans shall include step-by-step emergency procedures, including:

6.2.1.1. Identify relevant stakeholders (primary and secondary) and establish a call tree.

6.2.1.2. Conduct a damage assessment of the impacted IT infrastructure and apps.

6.2.1.3. Establish procedures that allow facility access (e.g., recovery/secondary site) in support of the restoration of lost data in the event of an emergency.

6.2.1.4. Recover critical department services and information assets based on recovery priorities as established during the BIA.

	<b>PINAL COUNTY</b> <b>Business Continuity and Disaster Recovery</b>		
	DATE: 08/26/2020 REVISED:	PAGES: 7	POLICY NUMBER: 11.005

6.2.1.5 Provide interim means for performing critical business processes at or above the minimum service level defined in the BCP and within the tolerable length of time.

6.2.1.6. Restore service at the original site of impact and migrate from the alternate locations to the original site without unacceptable interruption or degradation in service.

6.2.2. All Departments must ensure that DR plans shall be tested annually. The test may consist of structured walk-through exercises or actual execution of the plan at an appropriate alternate site. The results shall be discussed, reported and documented with senior management and the Information Security Department.

6.2.2.1. Detailed test plans shall be developed with clear test scope, purpose and objectives, as well as identify the personnel involved and the timeframe necessary for the test. Measurement criteria must be included.

6.2.2.2. Information security aspects (e.g., data protection) of the test plan shall be reviewed and approved by the Information Security Department.

6.2.2.3. All critical processes and applications/systems for contingency, recovery, automatic fail-over, manual fail-over and replacement of failed components shall be tested:


6.2.2.3.1. Annually under normal operating conditions. The assessment may include announced or unannounced events.

6.2.2.3.2. Whenever significant technological, organizational or business changes occur.

6.2.3. All Departments must ensure that DR personnel shall keep a current copy of the DR plan documentation at the designated primary and alternate locations.

6.2.4. All Departments must ensure that approval to distribute the DR plan is the responsibility of the designated DR Lead.

6.2.5. Systematic version control to manage the DR plan shall be implemented to maintain accuracy. Outdated versions of the DR plan shall be retired.

	<b>PINAL COUNTY</b> Business Continuity and Disaster Recovery		
	DATE: 08/26/2020 REVISED:	PAGES: 7	POLICY NUMBER: 11.005

## 7. CONTROL MAPPING

This chart is used to provide an efficient way to cross-reference this policy's components with the different industry standard information security controls.

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Business Continuity Management	AU-7	CSC 6	PR.PT-1
	AU-9	CSC 6	PR.PT-1
	IR-4	-	DE.AE-family
	CP-1	-	ID.GV-1
	CP-2	-	ID.AM-5
	CP-4	CSC 10	PR.IP-4
6.2 Disaster Recovery Management	CP-1	-	ID.GV-1
	CP-2	-	ID.AM-5
	CP-4	CSC 10	PR.IP-4
	CP-6	CSC 10	PR.IP-4
	CP-7	-	-
	PE-17	-	-
	CP-10	CSC 19	RS.RP-1

## 8. RELATED DOCUMENTS

Document	Effective date

## 9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
1.0	Jerry Keely	08/26/2020	Approved by Board of Supervisors