PINAL COUNTY Enriching Lives Beyond Expectation	PINAL COUNTY Third Party Information Security		
	DATE: 08/26/2020 REVISED:	PAGES: 9	POLICY NUMBER: 11.015

Third-party Information Security Standard

Table of contents

1. PURPOSE

1.1. This standard establishes security requirements for the use of third parties that handle Pinal County confidential information, either by storing, processing, transmitting or receiving information. This standard outlines the following controls to reduce the information security risks associated with contracted services and staff:

- Identification of risks related to third parties to ensure appropriate protection of county information assets
- Definition of information security requirements for third-party agreements
- Third-party information management oversight from contract initiation through termination

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 Pinal County departments and offices shall adhere to the policies, procedures and objectives established by the IT 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 of Pinal County including all boards, offices, commissions, departments, divisions, councils, and bureaus. Other County entities that voluntarily use or participate in services provided by the IT Security Department, such as Pinal.gov, must agree to comply with this document as a condition of use. Pinal County departments and offices are required to implement procedures that ensure their personnel comply with the requirements herein to safeguard information.

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 this standard and may enlist other departments and offices to assist in the monitoring and maintenance of 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 mailto:ITSecurity@Pinal.gov.

4.4. Additional information regarding this standard and its related standards may be found at https://www.pinalcountyaz.gov/HR/Pages/PoliciesProceduresRules.aspx.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all of Pinal County including all departments, offices, boards, commissions, 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 Information Security Office (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).

6. STANDARD STATEMENTS

6.1. Third-party Selection

As part of the third-party selection process, county departments and offices must ensure that the items listed below should be evaluated from a security perspective during the sourcing and contracting phases:

6.1.1. Technical and industry experience

6.1.1.1. Identify areas where the county may have to supplement the third party's capabilities related to information management to fully manage risk to the County's information assets.

6.1.1.2. Evaluate the third party's use of other third parties' (i.e., subcontracting relationships) technology to support the contracted operations.

6.1.1.3. Evaluate the experience of the third party in providing services that include the handling of confidential information in the anticipated operating environment.

6.1.1.4. Evaluate the third party's ability to respond to service disruptions (see Information Security Incident Management I-11.009 and Business Continuity and Disaster Recovery 11.005).

6.1.2. Operations and control (as applicable)

6.1.2.1. Determine/review the adequacy of the third party's policies and procedures relating to internal controls in accordance with Report on Controls of Service Organizations such as SOC1/SOC2 User/Client Control Considerations (e.g., parameters, logical access, event logs/audit trails), facilities management, privacy protections, maintenance of records, business resumption contingency planning, secure systems development and maintenance and county employee background checks.

6.1.2.2. Determine whether the third party provides sufficient security precautions, including, when appropriate, firewalls, encryption and customer identity authentication, to protect county information resources as well as detect and respond to intrusions.

6.1.2.3. Evaluate whether the county has complete and timely access to its information maintained by the third party both during and after any third party engagement.

6.1.2.4. Evaluate the third party's knowledge of regulations (e.g., PHI, PCI) that are relevant to the services they are providing.

6.1.2.5. Assess the adequacy of the third party's insurance coverage in consultation with risk management or procurement functions.

6.2. Contractual Security Risk Identification

All contracts by which a third party provides services to the county or allows a third party to access, store, process, analyze or transmit county confidential information shall be assessed, prior to entering into an agreement, to determine the third party's capability to maintain the confidentiality, integrity and availability of county information assets. The assessment process must be agreed upon by all stakeholders after the role in the supply chain is identified. The following shall be considered during third-party sourcing and/or contract negotiation:

6.2.1. Third-party sourcing and contract negotiation

6.2.1.1. Organizational objectives and requirements.

6.2.1.2. Transparency to evaluate and manage third-party relationships.

6.2.1.3. Importance and criticality of the services to the county (see Asset Management 11.004).

6.2.1.4. Defined requirements for the contracting activity, including any potential regulatory requirements.

6.2.1.5. Necessary security controls/reporting processes in county IT departments.

6.2.1.6. Contractual obligations and requirements to be imposed on the third party.

6.2.1.7. Contingency plans, including the availability of alternate third parties, costs and resources required to switch third parties upon breach or termination (see Business Continuity and Disaster Recovery 11.005).

6.2.1.8. Partners and suppliers critical information systems should be documented and prioritized.

6.3. Contractual Security Provisions

County offices and departments must ensure that Information Security policies and requirements are addressed and documented in any contract with the third party. Provisions shall be established in the contract to protect the security of the county's information assets.

6.3.1. Third-party contracts must address the following, where applicable:

6.3.1.1. All parties involved with the agreement must be made aware of their privacy and security responsibilities and are required to sign confidentiality agreements (e.g., non-disclosure agreement).

6.3.1.2. Relevant legal and regulatory requirements which may apply to information processed, stored or transmitted.

6.3.1.3. Requirements governing the acceptable use of county-owned or managed information.

6.3.1.4. The means by which a third party proposes to transfer information to other third parties and will require written notice and agreement from the county prior to any such transfer.

6.3.1.5. Adherence by the third party to an information security program, including, but not limited to, password and access management requirements, physical security of facilities and servers containing county information, network protection, system and software protection, encryption and information security of data in transit and at rest, and intrusion-detection/prevention systems.

6.3.1.6. Training and awareness requirements for specific procedures and information security requirements (e.g., for incident response, authorization procedures).

6.3.1.7. Screening requirements, if any, for third-party personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for concern.

6.3.1.8. Pinal County's explicit reserved right to audit the security policy and the performance of information security and other contractual responsibilities of the parties involved in the signed agreement. This will be done when deemed necessary by a county organization, and doing so will incur no additional cost to a county's contract.

6.3.1.9. Third party's obligation to periodically deliver an independent report on the effectiveness of controls (e.g., SOC1/SOC2, vulnerability testing results) and agreement on timely correction of relevant issues raised in the report.

6.3.1.10. Processes used by the third party to report incidents in writing to the county involving any type of security breach or unauthorized access to the county's information assets within the appropriate timeframes (see Information Security Incident Management Standard I-11.009).

6.3.1.11. Upon termination of the contract, county information will be transmitted to the county or the county's third party of choice in a format defined by the county at a cost specified to the mutual satisfaction of the county and the third party prior to termination.

6.3.1.12. Processes used to electronically erase, render unreadable or physically destroy all county's information assets upon termination of the agreement.

6.3.1.13. Pinal County's explicit reserved right to request, at any time, transfer or purging of some or all information stored on third-party systems at a cost specified to the mutual satisfaction of the county and the third party prior to termination.

6.3.1.14. Maintenance and testing procedures for Business Continuity Planning as appropriate.

6.3.1.15. Enabling processes to provide for timely forensic investigation in the event of a compromise.

6.3.1.16. When utilizing Software as a Service (SaaS) password requirements must meet at least the same standards as required by county policy for internal passwords and require two factor authentication.

6.3.1.17. Hosted SaaS systems must be able to be hosted on a county specified platform to meet county security standards and policy.

All contracts shall be reviewed by Legal for accurate content, language and presentation. If the information being collected or exchanged is confidential, a binding non-disclosure agreement shall be in place between the county and the third party, whether as part of the contract or a separate non-disclosure agreement (required before any confidential information is shared).

6.4. Third party Life Cycle Management

County departments and offices must ensure that all third parties shall be managed through the life cycle of the contract by the information owner in collaboration with the Information Security Team and Procurement/Legal.

6.4.1. The following shall be considered throughout the third-party life cycle management process:

6.4.1.1. Inventory of third parties with assigned vendor risk rating.

6.4.1.2. Contractual performance criteria or service-level agreements.

6.4.1.3. Contractual, regulatory or legal requirements.

6.4.1.4. Inventory of all relevant contractual deliverables.

6.4.1.5. Information classification of information entrusted to third parties.

6.4.1.6. Enablement of accounts used by third parties for remote access only during the time period needed and monitor remote access accounts when in use.

6.4.1.7. Audit provisions and continuous monitoring to determine the third party's compliance per defined requirements.

6.4.1.8. The frequency of audit based on advice from functions such as Internal Audit, Information Security and Legal.

6.4.1.9. Communicate the need for transition or return of information at end of engagement/contract and obtain certification in writing from the third party that all county information has been permanently deleted if the contract so requires.

6.4.1.10. Risk assessment at the onset and at least annually thereafter and upon significant changes to the agreement or environment. The risk assessment shall identify critical assets, threats and vulnerabilities and result in a formal, documented analysis of risk (see Risk Management Standard 11.010). Significant changes include:

6.4.1.10.1. Changes and enhancement to networks.

6.4.1.10.2. Use of new technologies.

6.4.1.10.3. Adoption of new products or newer versions or releases.

6.4.1.10.4. New development tools and environments.

6.4.1.10.5. Changes to the physical location of service facilities.

6.4.1.10.6. Subcontracting to another third party.

6.4.1.11. Awareness training for county personnel that interact with third parties regarding appropriate rules of engagement based on the type of third party and level of county information assets.

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 Third-party Selection	CA-2	CSC 4	ID.RA-1
	CA-3	CSC 1	ID.AM-3
	SA-9	-	ID.AM-4
	AC-1	-	ID.GV-1
	AU-1	-	ID.GV-1
	CA-1	-	ID.GV-1
	CM-1	-	ID.GV-1
6.2 Contractual Security Risk Identification	CP-1	-	ID.GV-1
	IR-1	-	ID.GV-1
	MA-1	-	ID.GV-1
	PE-1	-	ID.GV-1
	PL-1	-	ID.GV-1
	PM-1	-	ID.GV-1
6.3 Contractual Security Provisions	PS-1	-	ID.GV-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
	SA-1	-	ID.GV-1
	SA-6	-	-
6.4. Third-party Life Cycle	RA-3	CSC 4	ID.RA-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
		-	ID.AM-6
		-	ID.BE-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