Humboldt County

Countywide Information Security Charter

Document Control

This document is an internal, controlled quality record. The IT Information Security Officer is the owner of this document is the main author and is accountable for its contents.

Document Issue			
Project Reference	None	**Audience**	Internal
Owned by	Information Technology	**Approved By**	Board of Supervisors

Revision History			
Issue	**Release Date**	**Author**	**Amendment Summary**
V1.0	12/15/2020	TPL	Initial Draft
V1.1	TBD	TPL	Approved by the Board of Supervisors

1 Program Introduction

1.1 Purpose

This charter establishes a comprehensive security program to protect the confidentiality, availability and integrity of Humboldt County's informational assets.

Roles and responsibilities are outlined so all members of the organization understand their importance in information security.

1.2 Background - Importance of Information Security

One of the most important assets of a county government is its information, and the Board of Supervisors, County Administrative Officer (CAO), and Department Heads (elected and appointed) have legal obligations to make certain that such information is managed within the frameworks prescribed by law and regulation. The value and criticality of these informational assets require the implementation of a formal Information Security Program to meet these legal and compliance obligations. Major goals of the Information Security Program are to ensure and maintain the confidentiality, availability and integrity of the county's informational assets. Confidentiality means that information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of the data and data processing methods. Availability means ensuring that authorized users have access to data and associated information resources when required to perform their duties.

Humboldt County's informational assets include all data, in any form, and all data systems located anywhere within the County and hosted off-site. The diversity of these assets, and the foreign and domestic threats to them, complicate the task of information security.

The Humboldt County Information Security Program is based on principles established by the National Institute of Standards and Technology (NIST). These principles are promoted by the California Counties Information Services Directors Association (CCISDA) so that a level of trust and confidence can be achieved with all counties adopting these standards.

1.3 Mission

Humboldt County's Information Security Program provides a comprehensive structure of governance and operational functions to proactively protect the confidentiality, availability and integrity of the information the county uses and stores.

1.4 Scope

The Humboldt County informational assets include all data, in any form, and all data systems located anywhere within the County and hosted off-site.

All employees, vendors, elected officials, contractors, volunteers, business partners/associates and the Board of Supervisors are included in this program and have important roles in protecting the county's data.

2 Information Security Program

The goal of the Information Security Program is to meet the functional needs of the County in a secure manner by safeguarding the confidentiality, integrity and availability of the County informational assets at rest, in transit and in use. The specific components of the Humboldt County Information Security Program are described below.

2.1 Information Security Officer

This charter establishes an Information Security Officer (ISO). Under general direction from the IT Division Director, the ISO plans, organizes and directs the countywide Information Security Program, including IT security awareness, IT risk assessment, IT business impact analysis, IT systems recovery, and IT business continuity. The ISO is responsible for the day-to-day management of the County IT Security Team and countywide information security function.

2.2 Working Committee

The Information Security Working Group (ISWG) will be comprised of departmental representatives, in conjunction with the ISO, and will report to the IT Division Director. The ISWG will review and suggest updates to the Information Security Program and associated policies as necessary. Often compliance with security policies is lacking because the policies

are perceived as preventing an organization from performing its duties. The input of the ISWG keeps the policies and business goals in line. Policies are also implemented at a much faster pace because of cross-departmental involvement. ISWG members will also act as security champions for their respective departments. Departmental representatives will work with departmental managers, so all data and automated processes have designated owners. They will also participate in the development of department-specific information security policies and procedures.

2.3 Information Security Policies

The County's Information Security Policies set the stage for appropriate behavior, help staff process data securely, assist administrators in the implementation and configuration of new systems, and provide managers a means of determining if requirements are adhered to. Information Security Policies are developed by ISO, reviewed by ISWG & approved by IT, CAO, and Risk Management.

2.4 Risk Assessment

The ISO works with departments to assess information security risks and assist in planning for information systems continuity. This Information Security Program aims to move the County of Humboldt from a reactive response to a predictive model and secure the County assets before potential attacks are realized. Department Heads will make resources available to the ISO for risk assessment.

2.5 Data Classification

The County classifies information according to its sensitivity and the potential impact of disclosure. Access to information is provided when there is a business need following the concept of least privilege.

Data is classified to understand its requirements for secure storage and transmission. Data/Information Owners within departments determine classification for the data, and IT protects the data accordingly.

2.6 Security Awareness Training

The environment in which the county lives and works requires continual training in cybersecurity risks. Annual Security Awareness training is required of all employees, contractors, elected officials, interns, and volunteers with access to county information systems.

2.7 Monitoring and Assurance

Information security is a dynamic process that must be proactively monitored for the County to identify and respond to new vulnerabilities and evolving threats. The goals of the information security monitoring and assessment program include detection of anomalies and changes in the organization's environments of operation and information systems, visibility into assets, awareness of vulnerabilities, knowledge of threats, security control effectiveness, and security status including compliance.

The effectiveness of the County's security controls is measured by the use of industry benchmarks, external tests such as network penetration tests, audits of automated procedural controls, and vulnerability assessments, as examples.

3 Conclusion

Like any other countywide program, executive sponsorship and support are essential for this program's success. The Information Security Program is based upon Federal and State laws and regulations, and industry best practices. Furthermore, the adoption and unwavering support of this program allows the County to share informational assets with other counties, as well as with both State and Federal agencies that are mandated by law to comply with the same published standards. It is in Humboldt County's interest to adopt these standards proactively to deal with internal and external threats, as well as ongoing threats from foreign countries and entities that place information systems at risk daily.