Contents

1. Purpose

This policy provides guidance and defines the IT Security structure of County information and all IT resources. This policy is required to ensure compliance with State, Local, and Federal standards, regulations, and laws. Individual employees within the County will use the information in this policy as a guidepost and reference for how IT Security is practiced within the County and to what laws and regulations we adhere.

2. Applicability

This policy applies to all Buncombe County departments and employees. Where there is conflict with any department-specific policy, this document will supersede. This policy also includes and extends to IT systems and protections provided by vendors.

3. Policy

Protection of Buncombe County resident's private information and the County's significant investment in technology infrastructure is the foundation of this Policy. Effective and efficient delivery of County services is highly dependent on these information systems.

This Information Technology (IT) Security Policy reflects a common framework for the technical, procedural and management approach to protecting these assets and achieve the following:

3.1. Protect the County's infrastructure and the data we maintain, whether hosted by external entities (e.g. Cloud) or within County's data centers, from both internal and external threats.

3.2. Establish a countywide approach for Information Technology Security to maximize the functionality, security, and interoperability of the County's distributed information

technology assets, including, but not limited to, data classification and management, communications, and encryption technologies.

3.3. This policy includes all County information and information systems to include those used, managed, or operated by a contractor, or other organization on behalf of the County. This policy applies to all County workforce, contractors, and all other users of County information and information systems that support the operation and assets of the County.

3.4. **Frameworks, Requirements, and Controls** – The County adopts the National Institutes of Standards and Technology (NIST) Risk Management Framework, Special Publications (SP) 800-37, Guide for Applying Risk Management Framework (RMF) for Federal Information Systems as the standard for managing information. This policy is not intended to replace other regulations (such as HIPAA or CJIS) but complement them and provide a common approach to protecting County IT assets.

3.4.1. Life Safety System Protections – Buncombe County must implement controls to support the availability, integrity, and confidentiality of systems support public safety systems supporting life and safety of County residents, in accordance with State and Federal regulations and industry best practices.

3.4.2. Regulated and Sensitive Information Protection – Buncombe County must implement appropriate safeguards to ensure REGULATED and SENSITIVE information, including Personally Identifiable Information (PII), Protected Health Information (PHI) Federal Tax Information (FTI), Criminal Justice information (CJI), and Payment Card Industry (PCI) are protected from inappropriate disclosure, misuse, or other security breaches, in accordance with local, state, federal law and other security standards and requirements.

3.5. **Continuous Monitoring -** Continuous monitoring, automatic alerting, and assessment with corresponding tracking capabilities and reporting are required for devices connected to the County infrastructure or supporting County business (e.g. cloud services). The County must also have procedures in place to ensure robust incident response to unauthorized access and activities. The County IT Director has the authority to require the installation of monitoring or auditing agents on devices connected to the network.

3.6. **Security Architecture** - The County must implement appropriate information technology safeguards (such as encryption, data filtering, tagging, and segregation) to ensure highly regulated information is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with State, Federal and other security standards and requirements. Service delivery and IT support teams must ensure an appropriate response in the event of a breach of sensitive PII/PHI/CJI/FTI/PCI. consistent with Federal, State, and Local standards and laws.

3.7. **Roles and Responsibilities** - Providing a secure and effective operational business service is an integrated team activity. This requires active collaboration between the County divisions, county leadership, risk, compliance, and legal organizations, and the IT department throughout the life of the system. The roles and responsibilities identified below represent these entities to ensure security and compliance is achieved.

3.7.1. System Owner (SO) – System Owner defines the business needs, working closely with IT, Security, Privacy, Compliance, and other teams to define security requirements unique to the environment, including internal requirements and compliance driven needs.
3.7.2. Authorizing Official (AO) - County Manager or County Director understands and accepts the risk and responsibilities of operating a specific information technology system in support of County business goals and objectives.
3.7.3. IT Director (IT) – The IT Director provides the technical environment for delivery of technology in support of County business systems, including overall technical direction and architecture, application design and build, infrastructure engineering design and system build, as well as ongoing operational support and overarching administration of the County IT infrastructure.
3.7.4. Risk Officer (RO) – The County Risk Officer aligns the business risk management strategy with the business, technical, and operational requirements.
3.7.5. Privacy Officer (PO) – The County Privacy Officer maintains a deep understanding of the compliance and regulatory framework for operating County business and technical systems.
3.7.6. Chief Information Security Officer (CISO) – The CISO develops organization-wide technical security control strategy in close collaboration with business, risk, privacy, and IT resources. The CISO collaboratively implements and measures the effectiveness of this strategy through enforced security controls throughout the management, operations, and technical solutions within the county and a cyber-risk assessment and audit program.

4. Policy Non-Compliance

Employees willfully violating the terms and conditions of this policy may be subject to appropriate disciplinary action, up to and including dismissal and contract termination.

5. Audit

All policies for Buncombe County may be subject to audit or review as outlined in the Internal Auditor's Statement.

6. Definitions

6.1. **Data confidentiality** - Data Confidentiality deals with protecting against the disclosure of information by ensuring that the data is limited to those authorized or by representing the data in such a way that its semantics remain accessible only to those who possess some critical information (e.g., a key for decrypting the enciphered data).
6.2. **Encryption** - Cryptographically transform data to produce cipher text and is not readable by anyone not authorized.

6.3. **Framework** - A layered structure indicating what kind of programs can or should be built and how they would interrelate. Some computer system frameworks also include actual programs, specify programming interfaces, or offer programming tools for using the frameworks. A framework may be for a set of functions within a system and how they interrelate; the layers of an operating system; the layers of an application subsystem; how communication should be standardized at some level of a network; and so forth. A framework is generally more comprehensive than a protocol and more prescriptive than a structure.

6.4. **Information Assurance** - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

6.5. **Security Control** - A safeguard or countermeasure prescribed for an information system or organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

6.6. **Workforce -** Employees, volunteers, students, interns, temporary staff, contractors, etc., who perform services representing the county.

6.7. For a comprehensive list of Cybersecurity terminology and definitions, please see: https://csrc.nist.gov/glossary

7. Approval and Revision History

Policy Origination Date:	February 1, 2022
Requires Board Approval:	☐Yes ☒No
Board Approval Date:	Click or tap to enter a date.
Revision History:	September 2023 – added roles and responsibilities, removed 3.4, added life safety system protections section

8. Background

1.1. Cybersecurity has become a critical tool in protecting IT Assets and managing enterprise risk through avoidance, mitigation, or acceptance with the increased use of these systems to deliver services to the residents of Buncombe County.

1.2. Cybersecurity as a discipline and methodology continues to mature in terms of Management Frameworks, Knowledge, Skills and Abilities of Staff, Processes, and Technologies, where there are university degree programs focused on advancing these areas, with supporting technologies being developed within the private and public sector to support the needs of the business and governing law supporting the enforcement in specific use cases.

1.3. The introduction of Cloud systems and solutions allows for more flexible approaches to hosting and solutions but adds to the complexity and protection of systems within the environment and vendor hosted systems.

1.4. North Carolina Laws, Policies, and Guidelines

- Memorandum of Agreement (MOA) between North Carolina Health and Human Services and Buncombe County Health and Human Services (3/12/2021)
- [NC] Statewide security and privacy standards (§ 143B-1376(a)). https://www.ncleg.net/enactedlegislation/statutes/pdf/bysection/chapter_143b/gs_143b-1376.pdf
- State (NC) IT Security Policies: https://it.nc.gov/resources/cybersecurity-risk-management/initiatives/information-security-policies
- State (NC) IT Security Policies: https://it.nc.gov/resources/cybersecurity-risk-management/initiatives/information-security-policies
- [NC] North Carolina Local Health Department Accreditation (NCLHDA) https://nclhdaccreditation.unc.edu/

1.5. Federal References Laws, Policies, Directives, Regulations, Standards, and Guidelines

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) - Security Rule https://www.hhs.gov/hipaa/for-professionals/security/index.html
- Health Information Technology for Economic and Clinical Health (HITECH) Act https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
- Health Information Trust Alliance (HITRUST) common security framework https://hitrustalliance.net/csf-license-agreement/
- Code of Federal Regulations - 42 CFR Section 2 https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2
- Criminal Justice Information Security (CJIS) Security Policy https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
- Federal Tax Information https://www.irs.gov/privacy-disclosure/protecting-federal-tax-information-fti-in-integrated-eligibility-systems-ies
- Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/

1.6. Industry Standards and Guidelines

- Payment Card Industry Data Security Standards (PCI DSS) https://www.pcisecuritystandards.org/

1.7. Control Family Details

1. **Access Control (AC) -** Details around system standards, including account management, access enforcement, information flow enforcement, separation of duties, least privilege, system use notification, previous login notifications, current session control, session termination, security and privacy attributes, remote access, wireless access, mobile device access, use of external systems, information sharing, publicly accessible content, data mining protection, access control decisions, and reference monitoring.
2. **Awareness and Training (AT) -** Details around literacy and training, role-based training, training records, and training feedback.

3. **Audit and Accountability (AU) -** Details around event logging and management of all phases of audit records lifecycle maintenance.
4. **Assessment, Authorization, and Monitoring (CA)** – Includes system assessment, information exchange, plan of action and milestone, system authorization, continuous monitoring, penetration testing, and internal system connections.
5. **Configuration Management (CM)** – Establishment of baseline configurations, configuration change control, impact analysis, access restrictions for change, configuration settings, least functionality, system component inventory, configuration management planning, software usage restrictions, user installed software, information location, data mapping, and digitally signed components.
6. **Contingency Planning (CP) –** Planning, training, testing, alternate storage and processing sites, telecommunication systems, system backups, system recovery and reconstitution, alternate communication protocols, safe mode, and alternate security mechanisms.
7. **Identification and Authentication (IA)** – Including IA of Organizational Users, device identification and authentication, identifier management, authenticator management, cryptographic authentication, IA (non-Organizational Users), service IA, re-authentication, and identity proofing.
8. **Incident Response (IR) –** Includes planning, training, testing, incident handling, monitoring, reporting, response analysis, and information spoilage response.
9. **Maintenance (MA) –** Definition of performance of controlled maintenance, tools, non-local maintenance, personnel, timeliness, and field maintenance.
10. **Media Protection (MP)** – Definition of access, marking, safe storage, transport, sanitization, and downgrading.
11. **Physical and Environmental Protection (PE)** – Physical access authorizations, controls, transmission, output devices, monitoring access, visitor access, power equipment and cabling, emergency power, shutoff, lighting, fire protection, water damage protection, delivery and removal, alternate work sites, location of system components, asset monitoring and tracking, EMP protection, component marking, and facility location.
12. **Planning (PL)** – Development of System Security and Privacy Plans, Rules of Behavior, Concepts of operations, Security and Privacy Architectures, central management, baseline selection, and tailoring.
13. **Program Management (PM)** – Policy and procedure management of all aspects of the security program and all security families identified here across the entire lifecycle at all levels of the organization.
14. **Personnel Security (PS) –** Development of policies and procedures related to position risk designation, screening, termination, transfer, access and use agreements, external security, sanctions, and position descriptions.
15. **PII Processing and Transparency (PT)** – Authorities to process PII, purposes, consent, notice, categorization, and matching requirements.

16. **Risk Assessment (RA)** – Formalization of security categorization, risk assessment, vulnerability management, technical surveillance countermeasures, risk response, privacy impact assessments, critical analysis, and threat hunting.
17. **System and Services Acquisition (SA)** – Definition and formalization of allocation of resources, SDLC, acquisition processes, system documentation, security and privacy engineering principals, external system services, configuration management, testing and evaluation, process, standards, and tools, training, architecture and design, critical components, screening, unsupported system components, and specialization.
18. **System and Communications Protection (SC)** – Includes separation of systems and user functionality, share resources, denial of service protection, availability, boundary protection, transmission confidentiality and integrity, network disconnect, trusted path, crypto key management and protection, transmission of security and privacy attributes, PKI certificates, mobile code, secure name and address resolution services, technical protections and design standards including system partitioning.
19. **System and Information Integrity (SI)** – SI includes flaw remediation, malicious code protection, system monitoring, security alerts, function verification, software/firmware and information integrity, spam protection, error handling, information management and retention, and various techniques to ensure integrity.
20. **Supply Chain Risk Management (SR)** – Management of supply chain risk, provenance, acquisition strategies, supplier assessment, supply chain security, notification and agreement, tamper resistance, authenticity, and disposition.