BARNSTABLE COUNTY
INFORMATION TECHNOLOGY DEPARTMENT

Barnstable County

Information Technology Department

IT Policies and Procedures Manual

William Traverse, Director

July 20, 2023

Overview

This document provides guidelines in the form of policies and procedures for County employees and other affiliates to follow while using information technology systems or services owned or managed by the County of Barnstable, and for the secure use and safeguarding of data in its custody. It is the intent of the Barnstable County Information Technology Department (BCIT) to develop such policies and procedures to address potential operational challenges and concerns quickly and securely with appropriate remediation and corrective measures.

Careful consideration should be taken to verify that actions taken while fulfilling job-related or contractual responsibilities fall within the authorized parameters for access, utilization, distribution, and modification of technology resources outlined within this document.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will not be tolerated. It is the responsibility of each employee or affiliate of the County to familiarize themselves with these policies and procedures set forth herein prior to signing the agreement form at the end of this document.

Contents

I. Policies

a. Acceptable Use Policy

Overview

This policy establishes the acceptable usage guidelines for all County-owned technology resources including, but not limited to, the following:

Assets and Services Covered by this Policy

Workstations	Portable or desktop computers, docking stations, monitors, and other accessories (e.g., keyboards, mouse, headphones, etc.)
Portable Devices	Smartphones, tablets
Network Equipment	Firewalls, switches, network and communications cabling, wireless equipment
Audio/Video Equipment	Televisions, cameras, projectors, security equipment, cabling, printers, copiers, etc.
Software	Operating systems, applications, or computer programs
Services	• Telecommunications (e.g., voice, data/internet) • Software-as-a-service or subscription-based entitlements for services, social media platforms • Hosted infrastructure (e.g., servers, storage, websites)

Employees must not use County-owned technology resources in a way that disrupts business operations and/or the functionality of other users or compromises the security posture of the organization.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, including vendors. This policy applies to all equipment that is owned or leased by Barnstable County.

Policy

All County-owned equipment, network infrastructure, and software applications are the property of the County of Barnstable and therefore are to be used for official work only. Also, all data residing on County-owned equipment or services exists under the custody of the County of Barnstable and therefore and must only be used for official business and protected from unauthorized access or damage.

The following activities provide a general roadmap to use County-owned technology resources in an acceptable manner:

- Credentials (usernames/passwords) used to access County systems and services must be kept secure and protected from unauthorized use at all times.
- User accounts must not be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Employees are responsible for equipment assigned at hire, or at any other point during employment, and must take steps to prevent damage to equipment (intentional or otherwise), as well as from theft or loss.
- Employees may not store or transfer sensitive information, including but not limited to personally identifiable information or protected health information on unencrypted portable storage devices.
- Employees should not post or communicate from County held or hosted services publicly, in their individual or personal capacity.
- All devices connected to BCIT-managed services or networks by the employee or the County/IT, must maintain a sufficient security posture relative to virus/malware detection.
- Employees must use extreme caution when opening e-mail attachments or visiting links to websites contained in emails received from unknown senders. Scams, phishing e-mails, viruses, and malware are prevalent; scammers can mimic even trusted or recognized entities. When in doubt, contact Information Technology Department support personnel.
- Sensitive information, including, but not limited to, personally identifiable information, protected health information and personnel information, may not be transferred via electronic means without content encryption.
- Systems or services hosted from the County campus or other internal networks must always be accessed using a secure (VPN) connection when accessed remotely.
- All workstations should be kept secure; users should lock the workstation or log out of the workstation when not attended to protect unauthorized users from accessing secure files.

Employees may be exempted from these restrictions while fulfilling job responsibilities specifically under emergency circumstances with approval from County Administration.

Under no circumstances is a County of Barnstable employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing County-owned resources.

The following activities are **strictly prohibited**, with no exceptions:

- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of unauthorized or "pirated" software products that are not appropriately licensed for use by the County.
- Unauthorized use of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and copyrighted music.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server environments (e.g., viruses, malware).
- Revealing account passwords to others or allowing use of your account or password by others. This includes family and other household members, such as when work is being done at home or another remote location.
- Using County technology resources to actively engage in procuring or transmitting material that is in violation of harassment (sexual or otherwise) or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from a BCIT-managed user account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches, including but not limited to accessing data of which the employee is not an intended recipient or logging into a system or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Effecting disruptions of network communication for malicious purposes, including, but not limited to, network scanning, intercepting traffic, spoofing, or denial of service.
- Port scanning or security scanning is expressly prohibited unless it has been authorized by or performed by County IT staff for business purposes.
- Executing any form of network monitoring which will intercept or redirect data to a destination other than the original intended destination unless this activity is a part of an employee's normal job responsibilities.
- Circumventing user authentication or security of any host, network, account, or service.
- Interfering with or denying access to any services by other users unless this activity is a part of an employee's normal responsibilities. (e.g., IT personnel disabling a user account involved in a possible security incident.)

- Automating or scripting the sending of messages of any kind with the intention of disrupting the functionality of other users.
- Sending unsolicited email messages, including the sending of "junk" or "spam" email or other advertising material to individuals who did not specifically request such material, either internally or externally.
- Any form of harassment via email, telephone, or text messaging/chat whether through language, frequency, or size of messages.
- Engaging in non-County related business activities
- Engaging in political activities
- Unauthorized use, forging, or modifying of email header information.
- Solicitation of email for email addresses other than that the user's own account, with the intent to harass or to collect replies.
- Transferring County data to unauthorized devices and/or third-parties.

It is the responsibility of all County employees and affiliates to adhere to these rules as stipulated, and to report suspicious or untoward activity, emails, phone calls, or files to a direct supervisor and/or BCIT when questionable incidents occur.

b. Accessibility Policy

Overview

This policy establishes the accessibility guidelines for all County-owned technology resources, within the context of existing policies and procedures outlined in the *Barnstable County Personnel Manual, Appendix F*. The purpose of this policy is to ensure that all employees can adequately use the technology required for proper performance of their job duties. These types of accessibility requirements may include, but are not limited to, the following applications or devices:

- Screen reading software
- Screen magnification software
- Stereo headsets or other sound devices

This policy applies to all County-owned technology resources.

Policy

A reasonable attempt shall always be made to address the needs of employees, particularly when those needs are due to an accessibility issue presented by a physical impairment or disability. For more information refer to Barnstable County Personnel Manual, Appendix F.

Notice of accessibility needs is required as far in advance as possible, as turnaround time to provide accommodations may vary depending on the nature of a given request. Where a reasonable accommodation is necessary to enable persons with disabilities to perform the essential functions of their job(s), the County understands that an employee may be limited in

the amount of advanced notice that can be provided, but the County asks that employees with disabilities provide as much notice as is feasible given the circumstances.

Designated staff within BCIT will work with the Human Resources Department to ensure reasonable accommodations are met on a case-by-case basis.

c. Auditing Policy

Overview

This policy addresses IT personnel as well as third-party entities and their respective abilities to conduct information technology audits. An information technology audit is an evaluation of IT infrastructure, applications, data use and management controls against recognized standards to ensure adherence to existing policies, procedures and organizational goals.

Audits may be conducted to:

- Ensure integrity, security, confidentiality and availability of information and resources.
- Discover vulnerabilities in software or hardware that require mitigation.
- Investigate possible security incidents to ensure conformance to the established BCIT security policies.
- Monitor user or system activity where appropriate.

Policy

This policy covers all computers, equipment, services, and communication devices owned or operated by the County. This policy also covers any computers, equipment, services, and communication devices that are present on County premises, but which may not be owned or operated by the County of Barnstable. IT personnel or third-party auditors must not cause a significant disruption to any services at any time during an audit unless part of a planned maintenance window or downtime.

Access required to perform the audit activities will be permitted by County IT to the third-party on a case-by-case basis. County IT personnel will also inform any other internal stakeholders of third-party audits where appropriate, and when County IT personnel are conducting internal audit functions that are outside of a documented incident or regular periodic testing.

The access involved in an audit may include:

- User account access to any BCIT-managed system or service.
- Access to digital information that may be produced, transmitted, or stored on County equipment and/or managed services.
- Physical access to areas containing critical IT infrastructure.
- Access to interactively monitor and log traffic within County networks.
- External network perimeter penetration testing and port scanning.

The Barnstable County IT Department will identify a staff member to be available to assist in audits involving third parties. Audits performed by third parties must take place under a written service agreement which documents allowable dates for the audit activities to take place, with permission from the Director of IT or a designee a minimum of 24 hours prior to the test.

Exceptions may be granted under the following conditions:

- Audit actions are time sensitive, due to being part of the urgent investigation of an incident.
- Audit actions are required by law enforcement officials as part of an external criminal investigation.

d. Backup and Recovery Policy

Overview

The BCIT Department maintains systems and services to hold and retain all essential data for departments and employees. The most critical data resides within cloud service providers, which are contractually bound to assume the responsibility of backup, recovery, business continuity, and data integrity as part of their service offerings and adhere to service level agreements.

Data stored within these services are not susceptible to traditional means of corruption as files are not directly accessible, and exist in an append-only state, in which all changes to a file are committed to it as a new version of the file, with previous versions of the file always accessible. Additionally, data retention services provide a safety net where even deleted files that are inaccessible to users are indefinitely retained.

Cloud hosted server infrastructure is configured for regular backups within the service provider, as needed. The backup and recovery infrastructure, fault tolerance and business continuity mechanisms are delivered to the County as a customer by the service provider contracts which also include service level agreements.

Less critical or archive data is held on centralized storage devices on the County's internal network and managed by County IT staff. Backups for this data are performed between storage devices internally and replicated to a cloud service provider for archival redundancy.

The Barnstable County IT Department cannot guarantee the backup integrity of data stored on portable storage media, on devices under accounts not enrolled in cloud services or stored in locations that are not synced with cloud-based storage.

Policy

Individual departments and employees must store sensitive, important, and confidential data within designated cloud-based storage services. It is the responsibility of the department

manager to determine whether data is stored in a manner that is accessible to a group or restricted to an individual user.

The file storage services referenced within "*III.e. Supported Products and Services List*" are made available to employees and departments where appropriate.

Users logged into BCIT-managed devices will have common document folders automatically backed up, including "Documents" and "Desktop" folders, in addition to folders synchronized by default with cloud storage services.

Although file versioning and data retention services minimize the likelihood of actual data loss, users in need of assistance with file recovery should immediately inform County IT for assistance.

Restoration processes in these cases would rely on one of the following methods:

- Guided file version restoration by user
- Content discovery restoration by designated BCIT personnel

Barnstable County IT utilizes multiple network-attached-storage (NAS) devices on the main County Campus to store the following data types: See "*III.e. Supported Products and Services List*" for more detail.

- Archived data from on-premises servers created more than 7 years prior.
- Raw/unedited recorded footage from public meetings or other events, whose final form is also uploaded to online streaming services.

All NAS devices are configured to replicate to other storage devices on-campus and to cloud storage where possible and appropriate. Restoration of data stored in this manner requires file level access to copy replicated data manually to other storage devices or contacting the service provider and submitting a retrieval request.

Cloud-hosted server infrastructure that contains critical data is configured by BCIT to perform daily backups of critical servers and datasets in addition to backups performed by managed service providers.

Testing to ensure the reliability of the restoration process and integrity of data is handled by the vendors contracted to provide these services. Test restorations may be performed ad-hoc by IT staff where appropriate for training purposes.

Restoration processes for cloud-hosted servers would, as part of an incident response process, include one of the following methods:

- Restore to last snapshot of virtual server instance.

- Restore from database under guidance of service provider.
- Submit request to service provider to restore from disaster recovery data.

Log files containing information for backup or replication processes are reviewed for critical errors by BCIT staff where appropriate.

e. Data Retention Policy

Overview

This policy will determine how long data shall be retained under the guidelines of federal and state law and within institutional policies as dictated herein.

Policy

All data shall be retained, at minimum, for the time frame as specified in any current, standing federal or state law, and any applicable federal or state records retention requirements/ policies.

At present, the County of Barnstable maintains an indefinite retention policy for all data and will continue to do so, provided such methods continue to be cost effective. However, the County will ensure compliance with any record retention policy stipulated in a grant agreement.

No data shall be removed, discarded, disposed of, or otherwise destroyed without the necessary permissions having been obtained from BCIT. BCIT in conjunction with County Administration will ensure that permission from the relevant state agency(ies) is obtained prior to destruction of data that constitutes public record, where applicable.

The Barnstable County IT Department shall maintain an indefinite data retention timeframe for all data that is required to be accessed by the organization, without compromising legal statutes set forth regarding storage or destruction of such data. Under no circumstances is data to be removed, discarded, disposed of, or otherwise destroyed that will compromise legal compliance, data integrity, or organizational needs.

The Barnstable County IT Department will continually utilize services to ensure that critical data is retained and kept from corruption or other types of data loss.

f. Emergency Notification Policy

Overview

Barnstable County maintains an emergency notification system to notify employees, officials and others who have opted in. This system is updated with the onboarding or offboarding of personnel to ensure the list of those who are notified is as accurate as possible and is also periodically tested.

Policy

Emergency notifications are to be used for emergency purposes or purposes deemed necessary by County administration or their designees only. The notification system is to be used to send

messages via text to email addresses and mobile devices, as well as via voice to personal phones and cell phones.

At no time shall this system be used for normal communications and messaging, notifications, or otherwise standard contacts, unless permitted by County Administrator.

Tests of this system shall be conducted by designated staff annually to ensure the system is functioning properly. Additional tests may be conducted but are not required.

Only users defined below shall be able to send emergency notification messages via this system:

- County Administrator
- Assistant County Administrator
- Human Resources Director
- Designated IT staff
- Others designated by County Administration

Please refer to established procedures for the order of notifications under various circumstances or conditions.

g. Encryption Policy

Overview

The purpose of this policy is to establish security guidelines related to the use of encryption by County employees and affiliates while conducting business.

Policy

The County of Barnstable shall only engage with service providers that meet sufficient levels of industry-specific and/or governmental compliance. This includes the level of encryption employed in the delivery of such services. Service providers are responsible for identifying and providing the most up-to-date and standardized encryption algorithms for the following:

- Web based applications/services (e.g., software-as-a-service)
- End-to-end payload encryption services (e.g., email messages and attachments)
- Virtual private network/tunneling services (e.g., VPN software client of site-to-site hardware)
- Local storage (e.g., onboard storage of workstations/devices)

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by BCIT.

Although encryption at all defined levels provides adequate security against unauthorized access, users are ultimately responsible for protecting information from unauthorized access

while carrying out business. The following scenarios are means by which users can expose the organization to risk and should therefore be avoided:

- Leaving any storage device unattended that contains confidential data or a method to access confidential data, including publicly identifiable information (PII).
- Leaving a workstation unattended that has been signed in to and is unlocked.
- Permitting individuals to access a device or system containing sensitive information, unless they are authorized to do so as a service provider under an active service agreement, or another County employee whose job duties include working with such data.
- Attempting to disable or bypass encryption/security warnings when accessing systems or services.

Users must immediately report to BCIT any potential encryption/security warnings or errors they encounter while conducting business. Exceptions to this policy may only be provided under emergency circumstances and where risk of the exception is deemed minimal by the Director of IT or their designee.

h. Enforcement Policy

Overview

This policy establishes enforcement guidelines to ensure that all
Barnstable County IT Department policies and procedures are adhered to and observed by all departments and individuals including employees, visitors, and vendors.

Policy

Unless granted a specific exception, all policies herein are applicable to all users of technology resources at the County of Barnstable.

If it is determined that any individual, department, or external entity violates the policies and procedures set forth within this document, whether knowingly or unknowingly, then the enforcement of such policy may include, but may not be limited to:

- Revocation or limitation of certain access or user privileges.
- Usage of technological means to ensure compliance with policies.
- Disciplinary action up to and including termination of employment.
- Termination of vendor contract and/or service agreement.
- Prosecution to the fullest extent of the law.

Specific exceptions to various policies may be granted and documented as needed per the provisions of each individual policy.

i. Cybersecurity Incident Prevention and Response Policy

Overview

This policy is meant to establish how the County, through its Information Technology Department, shall detect and respond to cybersecurity related threats or incidents. Pertinent reporting requirements are outlined herein.

Policy

The County of Barnstable utilizes U.S. government-compliant cloud services for all core day-to-day business operations across all departments, including the processing and storage of electronic files that may contain sensitive data. The governance and management of these cloud-based services have been consolidated to qualified personnel within the Barnstable County IT Department. County IT staff are also responsible for technical support and incident response in areas beyond the purview of the service provider, as well as ensuring the following security measures are met:

- Services are utilized by staff in a manner compliant with applicable regulatory requirements, such as Criminal Justice Information Services (CJIS) security standards, and the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules, including the federal HITECH Act and its implementing regulations, as well as G.L. c. 93H.

- Access to all management systems utilizes a Zero-Trust security framework with multi-factor authentication. Requests for administrative access are reviewed ad-hoc by BCIT management, who confirm the validity of the task and subsequently allow or deny the request accordingly.

- Enhanced detection and response capabilities, regular system updates, and monitoring are implemented and up to date on all capable devices.

- All data at rest and in-transit is encrypted.

- No direct access shall be given to electronic files or file systems; all content is protected by retention policies.

Detection and Response

The BCIT employs the following measures to monitor and detect security events and data breaches in accordance with standards published under the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF):

- Weekly review and implementation of security and compliance recommendations from the service provider(s).
- Maintain near-real-time automated analysis of operations via service provider with notifications of potentially malicious behavior or possible security incidents which are sent to designated IT staff for review.
- Usage of data loss prevention services to detect and mitigate the dissemination, intentional or otherwise, of sensitive or personally identifiable information (PII) as defined in NIST Special Publication 800-122, to outside entities.

Reporting

Events that are either reported by personnel or detected automatically are investigated per incident by IT staff who may then take steps to mitigate while notifying the appropriate parties internally if needed, and externally to the extent required by applicable law, including state and federal law enforcement and/or regulators.

It is the responsibility of the BCIT director or designee to immediately contact County Administration and appropriate departmental management as soon as practicable under the following circumstances:

- To provide notification and further guidance related to a loss of service or service outage results in a compromised security posture.
- To report, confirm or further investigate a detected security event, including a suspected or imminent data/PII/PHI breach.

In the event a data breach has been confirmed, it is the responsibility of the BCIT director or designee to notify County Administration of the incident, which is to be reported to the following entities within 24 hours:

- Cybersecurity and Infrastructure Security Agency (CISA)/United States Computer Emergency Readiness Team (US-CERT)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Federal, state and local law enforcement officials, as required or necessary.

Response and Mitigation

Mitigation or remediation of confirmed or immanent PII data breaches or other major security incidents includes the following:

- The immediate deactivation and blocking of user accounts and/or services associated with employee(s) involved in the incident.
- Deactivation and/or wiping of physical devices that may contain sensitive data or materials.

Such actions may be taken preemptively, depending on the severity of the unconfirmed security event. Additional guidance or assistance may be sought from the appropriate agencies or contractors where appropriate.

j. Supported Products and Services Policy

Overview

This policy was established to standardize the procurement and configuration of County-owned technology resources, or technology resources intended to be purchased with County funding. The primary goal of this policy is to minimize the cost of support and maintenance by reducing the scope of supported products and services.

Policy

All departments and employees shall order and utilize equipment that is serviceable and approved by BCIT and compatible with services. To assist in this process, BCIT will maintain and provide a list of preapproved commonly needed product options for purchase. Equipment not on this list and greater that $250 in value may still occur with the approval of BCIT staff. This applies to all technology equipment including, but not limited to:

Hardware

- Workstations, either portable or desktop computers
- Smartphones/tablets
- Accessories (e.g., mouse, keyboard, cables, cameras, headsets, cases, stylus)
- Monitors/Displays/Audiovisual equipment
- Printers, Scanners, Fax machines and Plotters
- Copiers, Multi-Functional Devices
- Network Infrastructure (e.g., firewalls, switches, routers, wireless, data cabling)
- Specialized equipment, such as physical servers, storage appliances, etc.

Software

- Any application or computer program designed for use on County-owned hardware.
- Software licensing and annual support/maintenance

Services

- Telecommunications (e.g., voice, data/internet)
- Software-as-a-service or subscription-based entitlements for services
- Hosted Infrastructure (e.g., virtual servers or appliances, software-defined networking)

For more details on procedures required to place an order for technology equipment, please see the *IT Procurement Policy,* and *Supported Products and Services List*, included in this document.

k. Guest or Third-Party Access Policy

Overview

The County of Barnstable, as a public entity is inherently open to guests and visitors and may allow access to resources, if such access does not compromise the integrity of systems or services or violate acceptable use policy provisions.

Policy

Guest and visitor access shall be classified into three categories as described below:

1. **Guest**
   - Access granted to internet-only resources.
   - Public Wi-Fi networks only.

2. **Presenter**
   - Access to facilities and systems within shared spaces for the purposes of presenting to County employees or other groups as allowed by County Administration.
   - Access to conference room spaces and technology available therein.

3. **Contractor/vendor**
   - Supervised access to specific systems, data, or electronic files as part of a contractual arrangement with a vendor or third party.
   - Access determined by nature of service agreement with third party.

Under no circumstances should guests be given access outside of these scenarios unless granted permission by County Administration.

All vendors shall notify their contact of any work that will require access to internal networks, cloud infrastructure (e.g., virtual servers, networks, or storage) physical workstations/devices, or data. Upon being notified of access and confirmation of approval, BCIT will work with the vendor or contractor and provide credentials, if necessary, to allow minimal access required to fulfill their contractual obligations only.

Vendors or contractors performing work under contract for the County must comply with the County's *Acceptable Use Policy* and as such are expected to work in the best interest of the County.

I. Information Sensitivity and Classification Policy

Overview

This policy is intended to help employees determine how specific information is to be handled and/or disclosed to other parties, as well as the define the sensitivity of information that should not be disclosed outside without authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper, and information shared orally or visually (such as via phone and videoconferencing).

All employees should familiarize themselves with the information classification and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps to protect confidential information.

Training will be provided by BCIT periodically, with ad-hoc guidance as needed via IT support requests.

Questions about the proper classification of a specific piece of information Department Managers or their designees or BCIT.

Note that staff within individual departments are considered subject matter experts for their respective fields and are ultimately responsible for proper classification of the information they work with.

Questions about these guidelines should be addressed to the Director of Information Technology.

Policy

To assist employees in the proper classification of information, the Barnstable County IT Department employs data loss prevention tools from service providers which automatically detects and warns designated staff when access or transmission of sensitive information is initiated, such as:

- Bank account numbers
- Social Security numbers
- Credit card numbers
- Driver's license numbers

The guidelines below are meant to aid employees and increase overall awareness of the sensitivity levels of information they may be working with or exposed to while fulfilling job responsibilities.

The information retained by the County for business purposes can be divided into two distinct categories:

1. **Public Information**
   This is information that has been declared public information by someone with the authority to do so, or as defined by public records or open meeting laws and may be freely shared.

2. **Confidential information**
   This contains all other information, and although it varies in sensitivity level it should be protected in a more secure manner overall. Confidential information includes high sensitivity items such as personnel records, personally identifiable information, security related information and financial information. It also includes information that is less critical, such as internal working products or draft documents, which do not require as stringent a degree of protection and may be shared in a controlled manner if deemed appropriate.

County personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain regarding the sensitivity of a particular piece of information, they should contact their Department Manager or designee. If the information is not contextually specific to the department's area of expertise, Barnstable County IT may be contacted.

The sensitivity levels and descriptions below provide details on how to handle and protect information. Use these guidelines as a reference only.

Minimal Sensitivity
Disclosure of "Minimal Sensitivity" information poses little to no risk to individuals or the County.

Description	General/public information, access can be granted without limitation regardless of affiliation.
Examples	Staff directories, public websites, public records, general business information.
Access	County employees or contracted third parties as part of fulfilling work obligations.
Internal Distribution	BCIT-managed e-mail and file sharing services
External Distribution	BCIT-managed e-mail and file sharing services, public websites
Storage/at-rest	Do not allow viewing by unauthorized individuals. Do not leave data in a state that is accessible or unattended in any format. Protect data from loss, theft, or misplacement. Utilize individual access controls for intended recipients where possible and appropriate.
Disposal/Destruction	Data should be permanently expunged or cleared when disposing of equipment or storage media. Data retention policies and federal and state retention guidelines should be observed for original copies.

More Sensitive

Disclosure of "More Sensitive" information could cause limited harm to individuals or the County with some risk of civil liability. Usually subject to regulatory compliance.

Description	Financial, technical, safety, and most personnel/confidential information.
Examples	Employee records, IT service management data or configurations, public safety/security data or surveillance materials.
Access	Employees whose job functions necessitate the handling of such information. Third parties working within regulatory compliance, and under agreements for specific work.
Internal Distribution	BCIT-managed e-mail flagged as "Confidential" and BCIT-managed file sharing services.
External Distribution	BCIT-managed e-mail flagged as "Confidential", "View only", or "do not forward" and file sharing services, via private link for recipient and link expiration set.
Storage/at-rest	Utilizing individual access controls under an established platform for this information is highly recommended.
Disposal/Destruction	Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

Most Sensitive

Disclosure of information classified as "Most Sensitive" could cause significant harm to individuals and the County, including exposure to criminal and civil liability. Usually subject to legal and regulatory compliance.

Description	Operational, personnel, financial, and critical technical information related to organization-wide security.
Examples	Personally Identifiable and Protected Health Information, Social Security numbers, loan applications, IT security information, financial account numbers, IT security information/credentials.
Access	Only designated County personnel with approved access and dedicated user accounts for this purpose where appropriate.
Internal Distribution	BCIT-managed e-mail flagged as "Confidential" and BCIT-managed file sharing services.
External Distribution	BCIT-managed e-mail, sent as "Encrypted" and BCIT-managed file sharing services; shared via private link for recipient only, link expiration, and passcode enabled. Passcode communicated to the recipient verbally.
Storage/at-rest	Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.
Disposal/Destruction	A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines observed for original copies.

The use of non-BCIT-managed or third-party services to store or transmit any information is expressly forbidden, except where there is an established contractor responsible for compliance, or a third party is the primary custodian of the information. (e.g., account transactions with financial institutions via their secure services).

m. Identity Management Policy

Overview

To safeguard and ensure that the identities of individuals using IT systems are authentic and accurate, additional layers of security are required. These measures are mandatory for all user accounts in the form of multi-factor authentication (MFA). This requires a second factor (e.g., text message, app, phone call) that can be used to verify the identity of an individual attempting to gain access to any user account.

The Barnstable County IT Department is responsible for enforcing both password complexity and reset requirements, as well as multi-factor authentication requirements for all employees. This policy is applicable to all employees and third parties requiring access to County systems or data.

Policy

The County will adhere to a Zero-Trust security model where no unverified access to systems or resources is allowed, and no single factor of authentication will be trusted for user access. The following criteria govern the use of user accounts and the identities they assume, to better secure County systems and services:

- All BCIT-managed user account logins/passwords adhere to both password complexity and multi-factor authentication requirements automatically enforced by BCIT. See *Password Policy* for more information.

- Accounts not associated with centrally managed complexity requirements (e.g., logins for other services or third parties) will conform requirements outlined in the *Password Policy* and employ multi-factor authentication where possible.

- Authentication factors used for multi-factor authentication must never be methods that may be uniformly accessible to an individual attempting to gain unauthorized access.

- Administrative role assignment to user accounts must be approved by the Director of IT or their designee.

- All administrative user accounts must be separate/dedicated user accounts created in supplement to the individual's primary user account.

- Access granted to users must adhere to the principle of least privilege, where only the minimum level of access is granted to the resources needed to perform a given function.

- Administrative user accounts must utilize privileged identity management must be employed for administrative tasks which allow for approval-based access by IT management for the minimum time period required for such tasks.

It is the responsibility of employees to maintain secure credentials and protect from unauthorized access to all types of user accounts and equipment in a manner that is consistent with these criteria.

Selection and utilization of services must prioritize those with capabilities sufficient to meet these requirements.

Exceptions which may be made on a case-by-case basis for non-user accounts, such as the following, as approved by BCIT:

- Accounts used for automation services and employees are not permitted to log in to.

- Select administrative accounts that are only used for targeted purposes as required by service providers.

If an exception is made for a non-user account, said account will be restricted in whatever way possible from performing actions unrelated to its purpose.

Further exceptions may be made for pre-existing circumstances only on a temporary basis while an alternatives solution is explored and established.

n. Password Policy

Overview

Passwords are the first line of protection for all user accounts. Poor password selection can result in a decreased security posture for the entire organization. All County employees, contractors and vendors requiring access to County systems or data are responsible for securing their account properly with a strong password.

Policy

The password requirements assume the enforcement of multi-factor authentication (MFA) as outlined in the *IT Identity Management Policy*.

- Passwords for accounts and services managed by BCIT or, where possible, third-party vendors, must follow these guidelines:
  - Passwords must be at least 8 characters in length.

  - Do not use common words, phrases, or names that could be associated with an individual.
  - Do not consist of only a single word.
  - Multi-factor authentication is enabled on the account.
  - Do not re-use a password from any other login you possess.
  - Any documentations of accounts is done so securely, and only if necessary.

The following guidelines provide further detail on the safe handling of passwords:

- Passwords must not be inserted into email messages or other forms of electronic communication.

- Passwords may only be shared if authorized by BCIT, and only under circumstances where they will be reset shortly thereafter (e.g., new user onboarding, or in response to a security incident).

- Passwords should never be given out to anyone within or outside the County. This includes your supervisor, friends, relatives, or co-workers.

Credential vault platforms allow for the secure storage and sharing of passwords, credentials and/or other sensitive information. Such platforms available for use by County employees who need to manage and maintain multiple credential sets include:

- Credential management platforms, ideal for maintaining larger sets of information. See *Supported Products and Services* for more information.

- In-browser credential management – credentials may also be stored in web browsers for auto-completion if the following criteria are met:

  - The browser retaining credentials is on a County-owned and managed device.
  - Any account used to log into the browser to sync settings between browser instances is a BCIT-managed account.

o. Physical Security Policy

Overview

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. Varying degrees of security will be needed depending on the criticality of infrastructure at a given location.

Policy

All areas will be classified into four categories:

- Office space
- Remote office space
- Public/meeting rooms
- Restricted

Office spaces are areas within County-occupied facilities where employees work and fulfill job responsibilities. Access to these areas by non-employees must be limited and supervised in all cases.

Remote office spaces are areas outside of the County's immediate purview and may include private residences and/or shared telework spaces. It is the responsibility of the employee in these instances to prevent unauthorized access to County systems and data.

Public/meeting rooms are areas where shared technology exists to accommodate meeting functions, such as meeting presentations and audiovisual equipment. Meetings or functions held in these spaces must be permitted and supervised by County officials to protect shared assets accordingly. Access to County systems and data from equipment in these spaces is limited to prevent unauthorized access by members of the public.

Restricted areas are areas which contain significant IT infrastructure owned and operated by the County or a third-party vendor and where damage to such infrastructure would cause disruptions to services or compromise security. Examples of such locations include:

- Switch closets
- Server rooms
- Telecommunications rooms
- IT storage areas

All designated areas on County premises are physically secured by the Barnstable County Facilities Department, or the primary tenant of a given building.

Additional physical security for sensitive locations housing IT infrastructure is provided by locking equipment cabinets, or by security provided by a vendor providing hosted colocation space.

The final tier of security is to ensure that the information contained in such areas, be it on a transient or permanent basis, is encrypted and therefore inaccessible should the containing equipment be removed from the premises. Workstations or devices should not be left signed-in or unlocked. See "*Encryption Policy"* for more information.

p. Personally Identifiable and Protected Health Information Policy

Overview

This policy establishes the definition of Personally Identifiable Information (PII) and Protected Health Information (PHI) as it is maintained by the County and indicates what information may or may not be shared with third-party entities and under what circumstances.

Policy

This policy sets forth a process for evaluating and addressing the County's electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and PHI.

Personally Identifiable Information (PII) is defined as information about an individual that identifies, links, relates, or is unique to, or describes that individual. Such information may include:

- Names, personal addresses, phone numbers, birth date, birthplace
- Social Security Numbers, license numbers, bank account information
- Other specific family data such as maiden names, addresses, contact information, etc.
- Financial information such as bank account information, account balances, etc.
- Other information that, alone or in combination, is linked or linkable to a specific individual that would allow a person who does not have a personal knowledge of the relevant circumstances to identify the individual with reasonable certainty.
- Information requested by a person who the organization believes knows the identity of an individual to whom a record directly relates.

Protected Health Information (**PHI)** is defined as information that is created or received by the County and related to the past, present, or future physical or mental health condition of a patient, the provision of health care to an individual, and identifies the individual for which there is reason to do so. PHI includes information of a person both living and deceased.

Both PII and PHI must be handled with highest level of security possible and classified as "Most Sensitive" per the *Information Sensitivity and Classification Policy* and, as such, be protected from reasonably anticipated security threats, including risk of disclosure or unauthorized access to this information.

All County employees, including temporary or contract employees who have access to PII and/or PHI must take steps to identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of records containing PII or PHI.

The Director of Information Technology or their designee is responsible for working with stakeholders to evaluate the sufficiency of policies, procedures, PII or PHI systems, and other

safeguards in place to control its risks, revise or create new procedures to minimize risks, and implement regular monitoring to ensure the effectiveness of those safeguards.

Training will be provided by BCIT periodically, with ad-hoc guidance as needed via IT support requests.

q. Personal Technology Service Policy

Overview

This policy will define the guidelines by which BCIT personnel may perform support work on personally owned employee devices or other technology products. BCIT does not support or service technology for individuals who are not employees, elected officials, or otherwise affiliated with the County.

Policy

The Barnstable County IT Department wishes to both allow the targeted use of personally owned technology by employees and affiliates while limiting support expectations to a reasonable extent. County-owned/managed devices are fully supported by the Barnstable County IT department for all acceptable use.

Personally-owned devices may be allowed to access County systems and services securely; however, IT support is inherently limited due to the lack of manageability of such devices as well as the potential for devices to be non-standard, or not in the approved product catalog provided by BCIT.
A reasonable effort will be made to assist in accessing County services from personal devices if the device and required software itself is deemed compatible and is supported by the manufacturer.

Support of the device/hardware or software on the device that is not used to connect to County services will not be provided.

Guidance may be provided toward potential maintenance to correct the issue (e.g., updates, resetting) but not in-depth troubleshooting, or taking custody of the equipment to service/repair it.

r. IT Procurement Policy

Overview

The goal of the IT Procurement Policy is to have a simplified cost-effective procedure, for the acquisition, installation, and support of the County's computing environment. The Chief Procurement Officer and BCIT are responsible for assuring that the County provides a consistent manner for procuring, standardizing, maintaining, installing, tracking, supporting, and retiring of technology assets.

Policy

The Barnstable County Purchasing Division in conjunction with the County's Finance Department and BCIT are responsible for the acquisition of technology systems and related products.

This policy applies to all technology, County staff and departments who purchase technology, as well as the Cape Cod Commission where applicable, as defined herein.
It is the intent of this policy to achieve the following:

- Ensure that the Information Technology (IT) Environment to support the lease, purchase and implementation of IT related hardware, software, and services exists.
- Ensure that cost savings through enterprise or other aggregated purchasing mechanisms are identified and applied.
- Ensure the efficient and cost-effective deployment of information technology.
- Ensure that IT contracts, leases and purchasing guidelines are considered.

Assets and Services Covered by this Policy:

Hardware

- Workstations, either portable or desktop computers
- Smartphones/tablets
- Accessories (e.g., mouse, keyboard, cables, cameras, headsets, cases, stylus)
- Monitors/displays/audiovisual equipment
- Printers, scanners, fax machines and plotters
- Copiers, multi-functional devices
- Network infrastructure (e.g., firewalls, switches, routers, wireless, data cabling)
- Specialized equipment, such as physical servers, storage appliances, etc.

Software

- Any application or computer program designed for use on County-owned hardware.
- Software licensing and annual support/maintenance

Services

- Telecommunications (e.g., voice, data/internet)
- Software-as-a-Service (SaaS) or subscription-based entitlements for services
- Hosted Infrastructure (e.g., virtual servers or appliances, software-defined networking)

The procurement of hardware and software assets as well as services, must conform to the following guidelines for each category:

Hardware:

- All solicitation, including quotes for items greater than $250 dollars in value shall be administered and obtained by County Departments in conjunction with IT and Purchasing. The decision on computer system configuration resides with the Director of IT or their designee. A list of approved configurations will be maintained in a central catalog for use by departments.
- It is expected that all staff that require the usage and handling of County data or communication services have one County-owned computer system for work related functions and responsibilities.
- Smartphone/tablet devices require approval by the department manager or their designee.
- The purchase of standalone or unnetworked fax machines, printers and scanners require prior written approval by the Chief Procurement Officer.
- The purchase of desktop printers is prohibited unless a valid justification is provided by the requesting department and approved by the Chief Procurement Officer.
- It is preferred that all purchased computers and laptops minimally meet Electronic Product Environmental Assessment Tool (EPEAT) Bronze standard or higher where cost and performance needs will not be compromised. EPEAT criteria and a list of all registered products can be found at: www.epeat.net.
- It is preferred that all technology products minimally meet or exceed Energy Star certification where applicable and practicable. When Energy Star compliant products are not available, products in the upper 25% of energy efficiency as designated by the Federal Energy Management Program should be used.

Software:

- Software directly supported by BCIT is provided to employees by BCIT by default, or by request when quantities of licenses are limited. The selection of supported/available software is maintained by BCIT in a central catalog for use by departments.
- Requests for software must be submitted as work order requests to BCIT with justification. A license will be granted if available or procured if it is not.
- If the desired software is not immediately available as formally supported software, it will be evaluated for procurement under the following guidelines:
    - Functionality does not directly overlap with existing available software.
    - Compatible with County systems.
    - Supported by a known developer.
    - Integrated functionality with County access management and security.

Services:

- IT-related services are maintained centrally by BCIT and provided to staff/departments where appropriate.
- Requests for changes or additional services can be made to BCIT by work order will be evaluated accordingly.
- Software-as-a-service requests are evaluated under the same guidelines used for general "software" requests (IV, B, 3).

Variances and Exceptions to this Policy:

All variances or exceptions to this policy must be made in writing providing a justification of why a variance is required. The justification must be approved by the County Administrator.

Responsibility:

IT and Procurement staff are responsible for hardware recommendations, configuration, and quotes, per procedures listed below, in circumstances where special consideration is needed, IT and Procurement staff will coordinate as needed with departments to accommodate specialized technology needs.

For further information on the process of purchasing IT equipment via the Information Technology department, please refer to the *IT Procurement Procedure*.

For further information on equipment surplus processes, and disposal, please refer to existing policies established by the Barnstable County Chief Procurement Officer.

s. Device Management Policy

Overview

This policy establishes the means and methods the County of Barnstable, through its Information Technology Department, is to govern manageable technology assets for the purposes of security, support, and accountability.

Policy

To better support, secure, and track assets purchased with County funding, the Barnstable County IT Department has implemented a cloud-based device management system to maintain control over manageable assets. Such assets include, but may not be limited to:

- Workstations/laptops
- Tablet devices/Smartphones
- Other compatible computing platforms

Such assets or devices are to be enrolled into device management services in one of the following ways:

- Automatically, at purchase
  Where available BCIT will arrange for automated enrollment with resellers to avoid complications related to enrollments.
- By BCIT personnel
  For devices that are not enrolled by a reseller at purchase, BCIT staff will manually enroll the device upon receipt.
- By the end-user
  Because the possibility exists for devices to be used without being enrolled, either purposefully or accidentally, enrollment by the end user or recipient of a purchased device must be avoided outside of emergency situations, and exceptions noted where a capable employee does so under the guidance of IT staff.

The enrollment of eligible devices into device management services is mandatory within the *IT Deployment Procedure*.

The activity of managed devices may be monitored per the established *Auditing Policy*.

t. User Classification Policy

Overview

This policy establishes a framework by which County IT staff are allowed to support or provide technical resources to various individuals.

Policy

Due to federal regulations, individuals working as contractors (not employees with a contract) are not to be provided with dedicated County IT resources for purposes of creating their work product, such as workstations, user accounts, software, or licensing.

The following user categories may be affiliated with the County for various purposes at any given point. The list below itemizes these categories and outlines limitations for IT service provisioning.

- Full-time employees
- Part-time employees
- Seasonal/temporary employees
- Elected/appointed officials
- Contractors (third-party vendors)
- Volunteers/interns

Full-time County employees are considered information workers unless otherwise noted, and by default are the recipients of all services and consolidated licensing, with some possible exceptions.

Part-time employees by default will be provided with the same service level as full-time employees.

Elected/appointed officials are supported in a manner stipulated by the public body they are part of.

Contractors (third-party vendors) may be provided with limited services, and only in support of their contractual obligations. If access to systems or services is required that may present the contractor/vendor to the public or County employees through such systems, care must be taken to differentiate or make generic any communications.

Volunteers are to be treated similarly to contractors/third parties, with exceptions only made under special arrangements or emergency situations.

For more information on IT service delivery, please refer to the *IT Service Management Policy*.

u. Remote Access Policy

Overview

This policy establishes the guidelines and requirements regarding the use of remote access and the ability to manipulate sensitive information (including personally identifiable information), internal server applications, and other data from remote or off-site locations.

Policy

Any user who seeks to work off-site for the purposes of working from home or other private location, and is permitted to do so by their Department Manager and/or County Administrator, may use the following methods:

- Direct access to standard services such as voice/phone calling, email, file storage and collaboration, financial/ERP access, may do so securely with no additional software or configuration requirements.
- Access to systems such as GIS, facilities managed infrastructure, and Laboratory Information Management Systems.
- Access to other systems and services not available over the public internet or secured by BCIT-managed identities using establish virtual private network (VPN) software clients, provided by BCIT.

At no time should any information designated as "Most Sensitive" per the *Information Classification Policy* be transferred out of BCIT-managed services or systems to any other location.

Activity is monitored and regulated by cloud application security broker (CASB) services which allow IT personnel to monitor access and prevent the transfer of data to unmanaged locations. The employment of such cloud services and/or networking technology ensures that all systems and data are accessed in the most secure manner possible.

v. Incident Response Policy

Overview

This policy is intended to establish a framework for IT staff to follow when an event occurs that has a widespread impact on County information technology related services.

Policy

This policy will provide guidelines for incident response by designated personnel for the following categories of incidents:

Service outages

- Utility outages such as power or internet service regardless of cause.
- Limited or no access to critical business services such as email, phone, or files.

Cybersecurity incidents

- Any reported incident involving unauthorized access to an IT system or service.
- Any service outage determined to be caused by an individual.

Issues discovered and reported by any County staff member may be classified as an incident if the problem is determined to affect, or potentially affect, one or more work functions of the County that are critical for day-to-day operations. All incidents shall be documented as such as soon as the level of impact is verified.
Once an incident has been detected, designated IT staff members will take the following steps:

1. Open an internal IT Service Desk ticket.
2. Document who reported the problem and how it was identified.
3. Document the scope of the incident.
4. Inform IT management and stakeholders outside of IT, including department managers.
5. Director of Information Technology or their designee informs County Administration.

6. Depending on severity, IT will send affected users regular updates on the incident status, even if unchanged.

Once resolved and pertinent information gathered, a report will be composed by the IT Director or their designee and provided to County Administration within 24 hours containing the following elements:

- Summary of incident
- Detailed timeline of events
- Background/Commentary
- Corrective/Preventative Action Plan

Cybersecurity-related incidents will follow the above steps in supplement to the guidelines established in the *Cybersecurity Incident Prevention and Response Policy*.

w. IT Service Management Policy

Overview

This policy is intended to define expectations related to IT services provided by the Barnstable County IT Department.

Policy

The information technology department provides IT-related support services to all employees, elected officials and, to a limited extent, volunteers, and other affiliates or third parties. These services may be provided directly by department personnel or via a managed service provider.

Services provided by the department can be summarized by the following categories:

General Support	Technical help with supported technologies or systems, such as County-owned hardware, software, or services.
IT Change Management	Onboarding/offboarding of personnel, modification of permission or access controls to systems or data, or other changes to user accounts.
Incident Response	Urgent assistance outside of normal support channels, necessitating rapid action (e.g., security events, service outages, etc.).
Project Management	Implementation of systems or services which consist of many different tasks, and generally have impact on more than one department or function.

The Barnstable County IT Service Desk is available to field requests during normal business hours of 8:00 AM to 4:30 PM but are available 24x7 to field emergency requests from employees.

Contact information:

- Submit a ticket (Form) via BCIT's internal Sharepoint site
- Call (508) 744-1250; for emergencies, indicate that immediate attention is required.

The following turnaround times for responses and resolution can be expected for various tasks and priority levels, and any pertinent advanced notification if required:

Request Type	Response Time Goal	Activity	Resolution
Emergency	30 Minutes	Continuous effort	Patch/workaround
High Priority	One Hour	Continuous effort during business hours	Patch/workaround
General	24 Hours	Business hours	Patch/as needed
Onboarding	2 weeks, when advanced notice is given.		

Limitations to Support Availability:

Turnaround time

Support requests may take longer than anticipated due to extenuating circumstances, staff resource constraints, or surges to various types of tickets. It is the responsibility of IT staff to keep customers apprised of such situations and maintain communication regarding any potential delays.

Eligible personnel (see *User Classification Policy* for more information).

Due to federal regulations, individuals working as contractors (not employees with a contract, as defined by the Barnstable County Personnel Manual) are not to be provided with dedicated County IT resources for purposes of creating their work product, such as workstations, user accounts, software, or licensing. Exceptions may be made for cases where contractual work involves performing a service that necessitates secure access to County systems or data. In cases such as these, minimal access will be granted, and any accounts created must inherently identify the user as a contractor.

Note that the Barnstable County IT Department provides services externally for municipal customers under separate terms governed by individual contracts.

x. IT Move/Add/Change Policy

Overview

The goal of this policy is to provide guidance for all administrative IT actions that involve creation, modification, licensing, or deployment of IT resources.

Policy

The Barnstable County IT Department provides services as part of its regular support channel related to managing IT resources, such as user accounts, or hardware assets. These services can be categorized as follows:

- User account creation or modification
- Changes to access, account permissions
- Group, or distribution list memberships
- Licensing assignments, software installs
- Equipment Deployments

User account creation tasks usually occur at the start of an onboarding process but may occur as part of providing limited access to a contractor or other third-party. For more information please see: *IT Service Management*, *IT User Classification*, *IT Onboarding Procedure.*

Equipment deployments usually occur as part of an equipment deployment process.
For more information please see: *IT Deployment Procedure*.

All other changes regarding groups, access, licensing, permissions, or any change that increases the licensing entitlements, scope of permissions, or access to data or services, must be approved by the individual's department manager or authorized designee.

y. Electronic Signature Policy

Overview

This policy is intended to provide conditions for the provisioning and usage of electronic signature services for County employee and affiliates.

This policy applies to all employees, contractors, consultants, temporary, and other workers at the County, including all personnel affiliated with third parties or vendors.

This policy also applies to all related services managed by Barnstable County by or through its staff or third-party vendors.

Policy

All County employees or affiliates required to carry out business requiring secure electronic signatures (e-signatures) must do so using a BCIT-managed platform with access provided by the Barnstable County IT Department.

The Barnstable County IT Department is responsible for maintaining the appropriate services with third parties to securely meet the electronic signature needs of the County and its departments.

Employees requiring access to such services that have not already been provided them at onboarding by the nature of their job responsibilities, may request access from BCIT per the *IT Move/Add/Change Policy.*

Employees must use electronic signature services in a manner consistent with the *IT Acceptable Use Policy*. E-signature services must be used via County-provided/managed identities or credentials per the established *IT Identity Management Policy*.

Documents or other materials using personal credentials or accounts not associated with or managed by the County cannot be digitally certified as originating from County employees.

E-signature services indicated in "*Supported Products and Services List*" are provided to County employees and supported by BCIT.

Employees may be exempted from these provisions if approved by County Administration or BCIT management and only in such circumstances where said exemption is not sought solely for the purpose of convenience or familiarity.

z. Generative Artificial Intelligence Policy

Overview

The County of Barnstable recognizes the potential usefulness of language-model-based generative artificial intelligence (AI) applications and services. Such technologies are tools that leverage large data sets and machine learning to produce content based on user input.

In most cases, these tools will be delivered as part of an existing service to enhance user experience. (e.g. predictive text, automatically generated themes or intelligent information classification)

This policy applies to all employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, including vendors.

This policy also applies to all related services managed by Barnstable County by or through its staff or third-party vendors.

Policy

County employees are permitted to leverage generative AI technologies only through established service providers, either directly or as part of employed by service providers to enhance other services. Any usage outside of these services are not formally supported. In all cases, employees are responsible for the outcome regardless of the tool or technology that is being used to create, compose, or generate a work product.

Compliance with Legal and Regulatory Requirements

County staff must comply with all applicable laws and regulations governing the use of AI-based technologies directly or where it is indicated to be included within another service or toolset. This includes compliance with data protection and privacy laws, intellectual property laws, and anti-discrimination laws. The use of generative AI tools and applications must comply with the County's data privacy and data security policies.

Human Review and Approval

County staff must always review AI-generated material for inaccurate or incomplete information and / or non-compliance with policy or regulations. The employee is ultimately responsible for all content produced with the assistance of AI-based tools. The usage or source of generated materials should be disclosed when appropriate.

The County maintains access to such technology through existing Microsoft 365 service entitlements. BCIT places no restrictions on the rollout of generative AI-based features within existing products or services.

The Barnstable County IT Department is responsible for the further utilization or limiting of AI-based services and for providing access to County data for such purposes, as appropriate and in compliance with existing regulations or policies. Employees may be exempted from these provisions if approved by Information Technology Director or their designee and only for a targeted or limited purpose or task presented.

As this policy applies to a rapidly evolving technology, County IT will review and update terms and language to reflect changes to best practices and technologies as well as legal developments.

Usage of this and all related services are subject to the terms of the *IT Acceptable Use Policy*.

II. Procedures

a. IT Procurement Procedure

This procedure outlines how a County employee seeking to procure IT equipment may do so in a way that ensures the acquisition of fully supported/compatible devices.

1. Employee initiates the purchase of new equipment by starting an IT ticket via online form (available on the County intranet page) and selecting “IT Procurement”.
2. The IT procurement menu allows the employee to review pre-configured workstation packages, browse a list of pre-approved products, or, if they have the specific product information available, make a custom request.
3. Upon completion of the IT procurement form, IT staff receive, review, and approve the submission via a ticket within the IT service desk, and communicate with the requestor if any adjustments or modifications are needed.
4. IT staff will obtain a quote from the vendor for the products, provide it to the requestor and ask that a purchase order be returned.
5. Once the IT staff member is in receipt of the purchase order, the order is placed.
6. IT staff document the purchase order number and vendor order number for internal tracking and inventory.
7. Requestor is notified upon shipping of products.
8. Once delivered, IT staff unbox and check-in items.
9. Requestor is notified when all items in the order placed have arrived.
10. **Please refer to *IT Deployment Procedure* at this juncture.**
11. For devices and other manageable assets, IT staff reach out as part of a deployment ticket.
12. For other assets, IT staff reach out to facilitate pick-up of the item or delivery/setup.
13. Sign-off is obtained by IT staff either as part of a deployment ticket, at pickup, or at delivery.

b. IT Onboarding Procedure

This procedure outlines how new employee onboarding is handled from the perspective of IT services, specifically account creation and related tasks.

1. A personnel form is completed by the department hiring a new employee.
2. An approved personnel form is sent to the IT Service Desk as a ticket with a point of contact (PoC) indicated.

The following steps are performed by IT staff internally. The point-of-contact with the hiring department will be contacted directly if there are any questions or complications that arise throughout this process.

3. IT staff reach out to the PoC to confirm details about the new hire.
4. IT staff request further information regarding account permissions, and equipment.
5. Check for pre-existing accounts if the new user has previously worked at the County.
   - *If yes, and is in the same role, remove shared access to files or mailboxes that may have been created with a previous onboarding.*
   - *If yes, but in a different role, rename the pre-existing account if needed and proceed with normal account creation.*
6. If a predecessor is referenced, gather related information to use in account.
7. Confirm information gathered with department point-of-contact.
8. Create a user account; securely retain temporary credentials.
9. Add contact details to the new account, including employee type.
10. Apply group memberships.
11. Apply licensing as required.
12. Assign specialized access to non-unified systems/services.
    - *For Munis access, verify and assign department-specific roles.*
13. Contact department point-of-contact to book an in-person orientation with an IT staff member and confirm equipment to deploy.
    - *Note: Because user credentials are provided at IT orientation, this should take place prior to any HR orientation.*

Refer to *IT Deployment Procedure* at this juncture. The following steps continue, again by IT staff, under the assumption that the *IT Deployment Procedure* has been completed successfully.

14. Log in to the employee's device with temporary credentials saved from earlier in the process.
15. Verify all application installs and updates.
16. Verify predecessor configurations have been applied.
17. Contact department point-of-contact to schedule delivery and/or setup.

The following tasks are performed by IT staff at the start date, or as soon as resources required by a predecessor and/or any other business function can be reassigned to the new user account.

18. Predecessor phone number/call queue/auto-attendant setup.
19. Share predecessor resources with new user, as required.
20. Unhide new contact from internal lists, and share contact for public website listing and emergency alert setup.

The following tasks are performed at the new user's IT orientation:

21. Supply user credentials, assist with login and resetting temporary password.
22. Confirm multi-factor-authentication has been enabled and assist with setup.
23. Verify user access to email and Teams.
24. Introduce SharePoint and OneDrive.
25. Supply quick-reference guide via email with IT support contact information.

26. See IT Quick Reference Guide included with this document.
27. Verify printer and Wi-Fi access if needed.
28. Obtain sign-off for equipment from user.
29. Update inventory with ownership identity.

b. IT Deployment Procedure

This procedure outlines how IT staff deploy equipment specified in the *Supported Products and Services Policy* to County employees. This function is often coupled with either an IT onboarding request, or an IT procurement request.

1. A deployment ticket is created by IT staff under the following circumstances:
   - For newly purchased equipment
   - For used devices reassigned from other/former employees
   - Previously used but ready-to-deploy, having already been through the reclamation process

     *See *IT Reclamation Procedure* for more detail.

2. Department point-of-contact for deployment is verified.
   - This may be the point-of-contact established via the *IT Onboarding Procedure* for a new user, or the recipient of the equipment themselves if for an existing employee.

The following steps are performed by IT staff internally. The point-of-contact within the target department will be contacted directly if there are any issues or complications that arise throughout this process.

3. Log in to device with service account, verify connectivity.
4. Perform software updates, verify enrollment with device management services.

Refer to Step 16 of the *IT Onboarding Procedure* at this juncture if a deployment is part of an existing onboarding process.

The procedure may continue with the following steps, performed by IT staff, if deployment is NOT part of a new user/onboarding process:

5. Perform device reset.
6. Contact department point-of-contact to arrange for delivery and/or setup.
7. Obtain user sign-off for equipment upon delivery.
8. Update ownership information in IT inventory.

c. IT Reclamation Procedure

This procedure outlines how IT staff reclaim or repossess equipment from County departments or employees and prepare them for future use as required. This often follows an offboarding process for a terminated employee, and prior to deployment for an existing or new employee.

1. A reclamation ticket is created by IT staff to make-ready or prepare a piece of equipment for use by another employee.
   - This procedure is carried out in the same fashion regardless of the indented use of the equipment being reclaimed.
   - IT staff may supply inventory information to assist departments with collection.

2. Verify department point-of-contact for reclamation.
   - This will be the point-of-contact only for taking possession of the equipment to be processed by IT staff, and for any questions regarding the condition of said equipment.

The following steps are performed by IT staff internally. The point-of-contact with the department will be contacted directly if there are any issues or complications that arise throughout this process.

3. Verify availability of the equipment, if needed, with the point-of-contact.
4. Take possession of the equipment.
5. Verify functionality, check for damage.
6. The last individual in possession of the equipment is responsible for the condition of the equipment, unless previously reported.

The procedure continues under the assumption that the device is in good working condition. Note that the following steps apply to computers/workstations only. The following steps are carried out by IT staff:

7. Log in to device with device administration or equivalent account.
8. Ensure that there is no local data present on the device. If there is data on the device verify that it has been synchronized to cloud storage, if possible.
   - If data has not been synchronized or it is not possible to determine, copy local data to IT archive storage and consult point-of-contact.
9. Perform device reset.

   *Refer to *IT Deployment Procedure* at this juncture if required for an existing or pending deployment process.

The procedure continues below under the assumption this deployment is NOT part of an existing onboarding process. The following steps are carried out by IT staff:

10. Label device/equipment accordingly for storage.
11. Update ownership information in IT inventory.

d. IT Offboarding Procedure

This procedure outlines how the offboarding of a terminated employee is handled from the perspective of IT service personnel.

1. Personnel form is completed by the department offboarding the employee.
2. Approved form is sent to IT Service Desk as a ticket.
3. Immediate actions to be taken by IT staff at close-of-business on effective date, unless a more specific time is provided:
   - Reset Microsoft 365 account password.
   - Force sign-out.
   - Revoke multi-factor authentication sessions.
   - Force reset of multi-factor authentication methods.
   - Disable access to services with non-unified credentials.
   - Securely document reset password.

Note: from this point forward, any actions performed by or through this account are now considered to be action performed by IT staff with access to the reset credentials.

4. IT staff reach out to the Department point-of-contact to determine offboarding details. Refer to *IT Reclamation Procedure* at this juncture.

The following steps performed by IT staff continue in tandem with the *IT Reclamation Procedure*.

5. Verify safeguards for data retention are in place, including litigation-hold mechanisms.
6. Convert user account to shared mailbox account.
7. Adjust account contact information where appropriate, including employee type.
8. Contact department point-of-contact to confirm/obtain requirements for providing access to resources and redirection of communication.
9. Apply and confirm access with point-of-contact or designated user if necessary.
10. Remove group memberships and unassign licensing.

III. Standards

a. Supported Products and Services List

The following list itemizes products and services supported by the Barnstable County IT Department (BCIT), and the level of support that can be expected or provided related to them.

Software/Subscription Services

Microsoft 365 Government Community Cloud – Cloud-based productivity, communication, and security.

Barnstable County IT maintains an enterprise agreement for Microsoft services and plans renewals to meet the needs of all County employees. A reasonable quantity of licensing is purchased to accommodate for unplanned growth.

Functionality:

- E-mail, calendaring (Outlook)
- File storage, file sharing/collaboration (OneDrive/SharePoint Online)
- Productivity Applications (Word, Excel, PowerPoint, Forms, Bookings)
- Automation Tools (Power Automate, Power Apps)
- Data Analytics (Power BI)
- Phone, video conferencing, chat (Teams)

DocuSign – Electronic Signature Platform

DocuSign is renewed centrally by BCIT and is licensed by transaction, meaning there is no individual cost per user license.

Functionality:

- Electronic signatures
- Approval workflows
- Online forms, via web browser or mobile app

Munis (Tyler ERP) – Financial information system/Enterprise Resource Planning

Munis/Tyler ERP is licensed at a usage tier for the entire organization and does not require the purchase of individual licenses. Access to the system is governed by the Finance Department and configured by BCIT.

Functionality:

- Procurement
- Accounts payable, accounts receivable
- Budget entry
- Financial content management
- Payroll processing

Adobe – Design and productivity software (Limited availability)

Adobe products are renewed annually on a single account to maximize volume discounts. Although this service has been consolidated, additional licensing needs must be planned for and funded in advance or funded by individual departments as needed.

Functionality:

- PDF editing, PDF form creation (Adobe Acrobat DC)
- Publishing, graphic design, video editing/production (Adobe Creative Cloud)

1Password – Secure password management platform (Limited availability)

1Password entitlements are maintained per-user and increases to utilization must be planned as procurement may be required.

Services/applications available:

- Secure credential vault and sharing, via web browser, desktop, or mobile app.

Formstack – Online forms (Limited support)

Formstack entitlements are centrally managed. Additional licensing requires advanced notice for procurement purposes. However, due to the overlapping feature sets of other supported products, usage should be minimized if possible.

- Online forms
- Approval workflows

Specialized Support

The following platforms are specialized per-department and supported to varying extents by BCIT and outside vendors.

Laboratory Information Management Systems (LIMS)
Laboratory analysis and accounting software utilized by the Barnstable County Department of Health and Environment/Water Quality Testing Laboratory
ESRI ArcGIS
Geographic Information System Software utilized by the Cape Cod Commission.

Hardware/equipment

Workstations, laptops, tablet computers – Microsoft Surface
Smartphones, mobile devices – Apple iPhone, iPad

More product detail as well as compatible accessories and peripherals can be found in the IT procurement product list within the support request form on the Employee Intranet.

Infrastructure

Storage
Synology – Network attached storage (NAS) appliances (Physical hardware)
Microsoft Azure – Storage services (Cloud-based)

Network
Cisco Meraki – Firewalls, switches, and wireless access points (Physical hardware)
Cisco Meraki – Virtual firewall appliances (Cloud-based)
Microsoft Azure – Software defined networking (Cloud-based)

Servers/compute
Microsoft Azure – Virtual machines (Cloud-based)

Business continuity/disaster recovery
Microsoft Azure – Service level backup and redundancy
Microsoft 365 – Service level redundancy, data retention, and versioning
Tyler Technologies – Off-site replication of financial system (Munis) databases

Operating systems
Microsoft Windows-based/compatible, where applicable. (Microsoft 365 subscription)

Platforms

Device Management
TeamViewer – remote support and system management
Microsoft Intune – Device management and compliance (Microsoft 365)
Microsoft 365 Defender – Threat detection and response (Microsoft 365)

Voice calling/phone system
Microsoft Teams (Microsoft 365)

Enterprise Resource Planning
Tyler/Munis – Financial information management, disaster recovery/backup

b. IT Quick Reference Guide

This document serves as a concise listing of important online IT resources and reference tools available to Barnstable County staff.

Resources

- Office.com
  This is the site from which you can access the common Microsoft Office applications like Word, Excel, PowerPoint, and Outlook. You can also access SharePoint, Teams, and several other tools from this page via the menu in the top left corner.

- Employee Intranet
  Use this link to access the Barnstable County SharePoint site where departments share files with employees. The Human Resources documents you may need are found here.

- Tyler ERP
  Barnstable County uses this application for finances, including payroll and procurement.

- Employee Self Service
  Staff can log into Employee Self Service to review their available time off and update certain personal information.

- Barnstable County Website (capecod.gov)
  This is the primary website for Barnstable County. It contains information about our organizational structure, history, and purpose, along with updates about its activities.

- Barnstable County IT Service Desk
  Need help? Create a ticket or schedule an appointment.

Credentials

Your Barnstable County username and password are used to sign into several Microsoft 365 services along with a few other enterprise applications. Access to these applications is available through links in the “Waffle Menu” at the top left corner of the Office.com page.

You can reset your credentials at any time by visiting: https://aka.ms/sspr
Do not share your username and password with anyone, at any time, for any reason. IT staff can reset yourself password if direct access to your account is necessary, but this is uncommon.

IV. Disclaimer

This document and the policies and procedures contained herein will undergo regular review and modifications. Changes in these policies and procedures after the initial agreement signature date does not allow non-compliance or permit any activity contradictory to the modifications made after the initial agreement signature date. As with all County personnel and administrative policies, employees are required to remain current on the updated policies and procedures.

V. Policies and Procedures Manual Compliance

Employees are required to sign the form on the following page indicating that they have received the policies and procedures set forth within this document. All employees are required to read these policies and procedures and if they have any questions, they should contact the Director of Information Technology.

A copy of all signatures shall be maintained by Human Resources to ensure all employees have signed and agreed to the policies and procedures included herein.

An employee's signature on a previous version of this document does not exclude any user from being required to abide by any new or updated policies or procedures.

Upon successful approval of any changes or additions, a copy shall be made available for all employees so that any current employee may review new or updated policies and procedures. Any objections to approved policies, procedures new or existing, may be brought to County Administration.

Signed agreement with the terms of this document are compulsory for employment or affiliation with the County of Barnstable and the use of technology resources owned or managed by the County.

Employees may obtain a current copy of this document from the employee intranet sites of Human Resources or Information Technology Department at any time. A hard copy may be furnished upon request.

VI. Policies and Procedures Agreement Form

I certify, by signing below, that I have received and reviewed the policies and procedures contained within this document and agree to abide by these policies and procedures. I acknowledge that it is my responsibility to ask for clarification of any provisions of the policies and procedures that I do not understand.

Name (print): _____Date: _____

Title: _____

Signature: _____

VII. Review

The Director of the Information Technology will review these policies and procedures at least annually, or in accordance with individual policy terms, to ensure content remains relevant and appropriate. Other materials and content may be adjusted as necessary.

VIII. Exceptions

The Director of Information Technology, with the approval of the County Administrator or their designee, may grant exceptions to specific terms within this document to accommodate for emergency needs, or maintain critical business operations in cases where such an accommodation does not present a security risk.

IX. Updates/changes

Draft created July 2023 – William Traverse, Director of Information Technology
Finalized August 2023 – William Traverse, Director of Information Technology