City of Dunwoody Georgia

4800 Ashford Dunwoody Road
Dunwoody, Georgia 30338
dunwoodyga.gov | 678.382.6700

To: Members
Dunwoody City Council

From: Ginger LePage
Technology Director

Re: Technology Policy
Date: 9/26/2022

Action

Adopt the attached Technology Policy for the City of Dunwoody effective immediately.

Summary

The proposed Technology Policy is a set of guidelines concerning technology issues system-wide. All previous policies were internal only and this would be the first adopted by City Council.

Details

This proposed Technology Policy would cover all major areas of the technical environment. Additionally, it can be used as a stepping stone towards accreditation with some entities in the future. Major areas that this policy addresses include:

* Regulating account management which includes procedures for regular audits, creation, and termination of user accounts.

* Overseeing remote access including requirements and authorization procedures.

* Authorizing equipment including devices such as cell phones, laptops, and tablets.

* Creating procurement procedures to ensure all new technology in the City's environment is properly vetted before purchase.

Note: No purchasing procedures will be overriden by the Technology policy, it may only make it more strict.

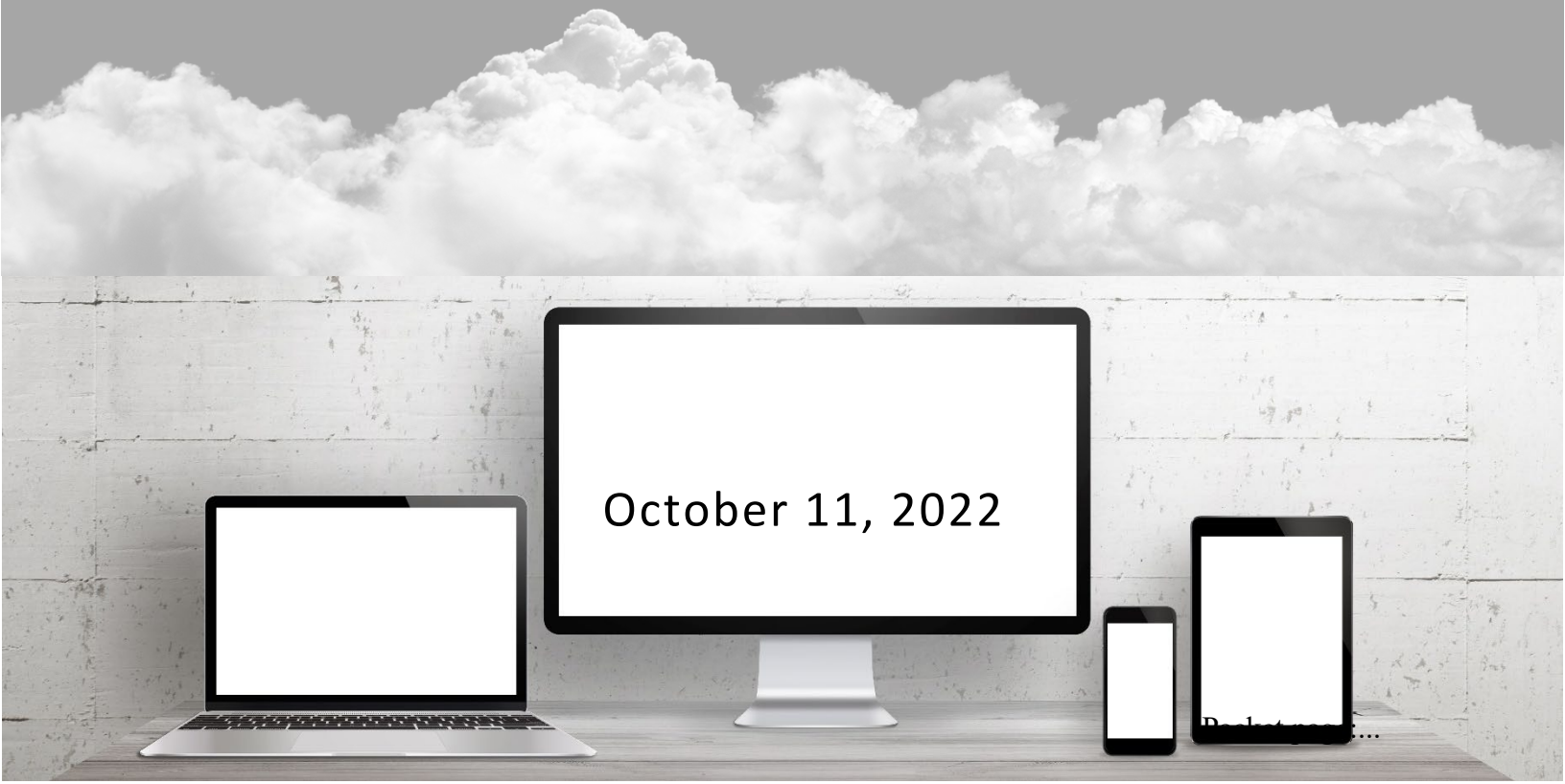
Recommendation

Adopt the attached Technology Policy for the City of Dunwoody effective immediately.

City of Dunwoody

Technology Policy

22. v1



October 11, 2022

TABLE OF CONTENTS

DOCUMENT VERSION INFORMATION

Version			
Version	**Date**	**By**	**Changes Made**
22. v1	10/11/2022	Ginger LePage	Final Approved

TECHNOLOGY DEPARTMENT PERSONNEL

Name	Designation and Role	Phone Extension	Hours available
Ginger LePage	Technology Director, Dunwoody	6781	M-F 7:30a-6p
Jordan White	Technology Manager, Dunwoody	6779	M-F
Michael Chamberlain	Systems Engineer II, Interdev	6782	M-F 9a-6p
Andrew Hulsey	Systems Administrator II, Interdev	6783	
	IT Support Specialist, Interdev	6784	
Justin Rowell	GIS Analyst II, Interdev	6815	M-F 8a-5p
Samira Hampton	GIS Tech, Interdev	6817	M-F 8a-5p
Andy Summers	PT GIS Manager, Interdev	6822	Tues
Neil Matchan, Danish Ali, Kendrick Cole, Sidney Smith	PT Security Engineer, Interdev	6785	Wed and Thu

The Technology Department consists of Engineers, Security, GIS, and Support Staff.

IT SUPPORT CONTACT INFORMATION

1. **After -hours IT emergencies (system down, software outage, major event, etc.) are reported via: 678-382-6799, option 2. This will route you directly to the IT Team member that is on-call. If no one answers, it will route you to secondary on-call person. If no one answers there either, it will route you to after-hours voicemail to leave a message (it will be delivered via email to the entire IT Services Team.) If you don't get a callback within 15 minutes, you can call back and select option 4 (this will route you to IT Management).**
2. **Urgent technical support during business hours are reported via: 678-382-6799, option 3.**
    a) This number rings all IT Staff phones for available team member to answer the phone.
    b) If no one answers the phone, leave a voicemail which will be sent via email to all IT staff
3. **For any non-urgent IT needs, users should email it.support@dunwoodyga.gov to create a ticket in the Helpdesk system.**
4. **Users can see all their open tickets by going to: https://interdev.myportallogin.com/ and choose to "sign up". Then, confirm email. After the email has been confirmed users can go to: https://interdev.myportallogin.com/ and either:**
    a) Submit a ticket or
    b) Lookup submitted tickets

IT TIPS AND TRICKS

1. The IT Department regularly sends out a pdf called "IT Tips and Tricks". This document holds the most frequently asked questions and should be checked before submitting a ticket. It includes information like:
    a) How to record your voicemail message
    b) How to reset your password
    c) How to know your password is expiring
    d) How to schedule a Microsoft Teams meeting

GENERAL INFORMATION

For the purpose of these policies and procedures:

a) The City of Dunwoody will be referred to as "the City"
b) "User" is any City Employee, Contractor, Vendor, Temporary Staff, and/or any other individual accessing City-Owned or Managed Technology Resources
c) Technology and "IT" will be interchangeably used

If a user is aware of another user violating any of these policies, procedures or other misuses, they should contact their immediate supervisor, director, or IT Management.

All policies were created based on compliance standards for National Institute of Standards and Technology (NIST) Special Publication (SP) and Criminal Justice Information Services (CJIS) Security Policy.

TECHNOLOGY POLICIES

IT-1 Account Management, Access Control, and Authentication

I. PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to the City's Technology resources and that proper access controls are implemented both physically and digitally.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all systems developed by, or on behalf of the City that require authenticated access. This includes all development, test, quality assurance, production, and other ad hoc systems. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

Account management and access control includes the process of requesting, creating, issuing, modifying, and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

V. POLICY

1. Identification and Authentication

IT Department shall:

a) Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of the users.
b) Ensure that information systems implement multi-factor authentication for network access to all accounts.
c) Ensure that information systems implement multi-factor authentication for local access to privileged accounts.
d) Ensure that information systems implement multi-factor authentication for remote access to privileged and non-privileged accounts.
e) Ensure that information systems implement replay-resistance authentication mechanisms for network access to privileged accounts.

2. Device Identification and Authentication

IT Department shall ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

3. Account Management

Account Management is the responsibility of the City Departments and the Technology Department working together to ensure accounts and access are updated immediately.

a) **Creating New Accounts:** To create an account, there must be a valid access authorization based on an approved business justification and a request must be made to create the account. New account requests should be routed from the Department Head (or designee) to Human Resources and then to the Technology Department with a minimum of five (5) business days advanced notice and preferred ten (10) business days, when possible.
b) **Enabling Access:** Access is granted, based on the principle of least privilege (ex. no local administrative rights), with a valid access authorization.
c) **Modifying Access:** All access modifications must include a valid authorization from the Department Head or City Management. When there is a position change (not including separation), access is immediately reviewed and added or removed based on necessity with Department Head or City Management approval.
d) **Disabling Accounts/Removing Access:**

i) **Event/Risk Based (Administrative Disable):** When an account poses or has the potential to pose a significant risk (ex. Inactive accounts, hacked account, disgruntled employee), either the account is disabled and/or access attributes are removed upon discovery of the risk. In this scenario, access can be re-enabled and restored once the risk is resolved.

ii) **De-provisioning Upon Separation:** Department Heads (or their designee) are responsible for notifying Technology Department immediately upon employee separation. This includes temporary employees, contract employees, and City employees. All user accounts (including privileged) must be disabled immediately upon separation. In addition, credentials must be revoked, passwords reset, and access attributes removed.

e) **Reviewing Accounts and Access:**

i) Accounts must be audited at minimum every six (6) months to confirm systems are accurately maintained.

ii) Access to privileged accounts must be audited monthly to determine if privileged access is still necessary.

iii) Inactive accounts may be automatically disabled after six (6) months of inactivity (if not being used as a site access only account),

iv) All users account access will be monitored.

f) **Process for Account Audits:**

i) Every six (6) months, an Electronic Audit Report for each Department will be generated by the assigned Technology Team Member.

ii) The Electronic Audit Report will be reviewed by each Department's Head or their assigned designee (Reviewer).

iii) The Reviewer will document any necessary changes, sign off on the Report, and return to the Technology Team Member.

iv) The Technology Team member will make any necessary updates to the system based on the Reviewers feedback and sign off on the Report.

v) The Report will then be submitted to Technology Management for final review and signature.

vi) The Final Electronic Report will be stored in Unity Client for permanent records.

g) **Unlocking User Accounts:** For an account to be unlocked, the user should make the request via phone or in-person to confirm the user's identity.

h) **Inactivity Lock:** Sessions must be locked after a maximum inactivity period of ten (10) minutes. After the inactivity period, the device will lock and require the user re-authentication to unlock.

4. Passwords

a) Passwords are an important aspect of computer security

b) All user-level and system-level passwords must conform, at minimum, to CJIS guidelines:

- Be a minimum length of eight (8) characters
- Not be a dictionary word or proper name
- Not be the same as the User ID
- Expire within a maximum of 90 calendar days
- Not be identical to the previous ten (10) passwords
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered

c) If at any time a user cannot construct a password that matches these criteria, the IT Department will assist

d) Users must use a separate, unique password for each of their work-related accounts (except for Single Sign On Accounts) and those passwords must not be used for personal accounts

e) If any user believes their password has been compromised, they should reset their password immediately and contact the IT Department.

f) Password cracking or guessing may be performed on a periodic or random basis by the IT Department or assigned designees. If a password is guessed or cracked, it must be immediately changed.

g) The City issues a Password Manager to all users to give them a secure way to store passwords. As such, passwords should not be written down, left in a plain text file, notes or excel documents, or left in any other easily accessible location

h) Individual User Passwords are not to be shared with anyone, including supervisors and coworkers

i) In specific scenarios where Technology systems require shared accounts and/or per IT request, passwords can be shared via Password Manager or a specified method as designated by IT Management

j) Passwords should never be sent via email, passed around via sticky note, added to tickets, or sent via any other electronic method (texts, teams, etc.) but instead, share the password utilizing the Password Manager application or a specified method designated by IT Management

5. New User Request Procedures

a) All requests to create a new user must include Department Head and HR approval in writing before the request is made to IT,

b) Once Department Head and HR have approved, the request packet (including all necessary approvals) should be emailed to it.support@dunwoodyga.gov,

c) When possible, to save time, include a user that the access rights can be copied from in the request packet,

d) All requests should be sent to IT with a minimum of five (5) business days before start date but preferred ten (10) business days advanced notice,

e) If the request is not made with a minimum of five (5) business days advanced notice, the account and any necessary technology will not be available by the start date.

6. Terminated User Request Procedures

a) All requests to terminate user access should be made as soon as possible,

b) If the termination date is in the future, include that date in the email,

c) All requests to remove users should be emailed to it.support@dunwoodyga.gov

d) Even temporary users need to be removed from the system as soon as their access is no longer needed

e) All requests must copy the HR Department as part of the request packet

f) If the request is made during after-hours, for access that needs to be removed immediately, call the After-Hours number at 678-382-6799, option 2.

IT-2 Electronic Message and Internet Usage

I. PURPOSE

To define rules and requirements for handling of electronic messages and internet usage regarding City networks and business systems.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all systems developed by, or on behalf of the City, which utilize electronic messaging. This includes all development, test, quality assurance, production, and other ad hoc systems. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

This Policy applies to the use of information, electronic and computing devices, and network resources to conduct City business or interact with internal networks and business systems, whether owned/leased by the City, the user, or a third party including the use of internet and email access. Teams is the preferred method of communicating via “messaging system”.

V. POLICY

1. Open Records:

All electronic messages from one computer to another whether through Mobile Computer Terminal (MCT), internal City Network, soft phone application, electronic messaging, text message, internet or other systems are subject to public records and the user should have no expectation of privacy or confidentiality. Every form of message is recorded and stored in compliance with Georgia Open Records laws. These records are all Public Record, therefore, the public, news media, judge, and jury could read and/or hear it.

2. Improper Use:

Internet access is a City resource and electronic messages are considered a work product. These services should be used to facilitate City business. Improper use of City managed electronic resources is strictly prohibited.

a) **Improper use includes:**

i) The use of City electronic messaging services, computer hardware, software, internet access, on-line services, and similar communications and information services for personal purposes.

ii) Not abiding by copyright, contract, or other local, state, or federal laws, administrative regulations, and individual department policies

iii) Intentional use of internet resources to access, transmit, or retrieve any material or communications that are obscene, pornographic or sexually explicit, of discriminatory or harassing nature, derogatory to any individual or group or are threatening in nature

iv) Offensive jokes, frivolous messages, or anything which is, or could be considered as, discriminatory in nature (refer to the employee handbook for additional information)

v) Intentional use of the internet to access, transmit, or download files that are knowingly dangerous to the integrity of the City’s network

vi) Use of internet resources for anything outside of City-related business

vii) Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware)

3. Emails

Users are prohibited from automatically forwarding email to a third-party email system without approval from IT Management. Individual messages which are forwarded by the user must not contain confidential information. Unless given written approval from IT Management, users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct business, to create or memorialize any binding transactions, or to store or retain email on behalf of the City. Such communications and transactions should be conducted through proper channels using City-approved documentation. Users should never add non-City email to City-Owned devices or City email to non-City devices without prior written approval from IT Management.

4. Audits

All department computer equipment, files, and all electronic communication are subject to audit and review for compliance. The City reserves the right, at its discretion, to monitor Internet and electronic mail usage patterns, without prior notice, to the extent necessary to ensure that the system is being used in compliance with this policy and other local, state, or federal laws. (ie: site accessed, on-line duration, times of day accessed, inappropriate messages).

5. Additional Considerations

a) All users are held accountable for use of their internet and electronic mail accounts; individual users can be held accountable for use of their accounts by others
b) Users are responsible for ensuring their emails, documentation, messages, and all other transmissions are professional, always.

IT-3 Acceptable use of Technology Resources

I. PURPOSE

To outline the acceptable use of computer equipment at the City. Appropriate organizational use of technology resources and effective security of those resources require the participation and support of all City users. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all technology resources that are owned or leased by the City and all employees, contractors, consultants, temporary staff, and other workers at the City. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organization's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible. The City may impose restrictions, at the discretion of Technology or City Management, on the use of a particular IT resource (ex. Block access to websites not serving legitimate business purposes). Users accessing the organization's applications and IT resources through personal devices must only do so with prior approval or authorization from Technology Management.

V. POLICY

Each user shall be responsible for the good care of City property whether assigned to them or available for them to use (including items assigned to individuals, items assigned based on position, and all other equipment owned by the City). The user shall promptly report to their Management the loss of, damage to, or outage of any and/or all such property.

1. Usage
   a) Storing any City data, including email, on a device that is not City-owned is strictly prohibited without approval of IT Management.
   b) Storing non-City data, including external email, on a device that is City-owned is strictly prohibited.

2. Personal Device Authorization:
   a) Any user with business need to use a vendor, contractor, or other non-City issued device should email the Technology Director. The initial email should include:
      i) Who owns the device?
      ii) What is the business need?
      iii) If the device is a computer, what anti-virus software is installed on the computer?
   b) The Technology Director will review and determine if there is a valid need for the non-City issued device.
      i) If the need is determined to be valid, the Technology Director will consult with the Technology Team and Security Team to ensure the device meets current City security requirements.
      ii) Most devices will likely not have a valid need for City access.

3. Acceptable Use:

All uses of technology resources must comply with organizational policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws (including Federal, State, local, and intellectual property laws). Consistent with the foregoing, the acceptable use of technology resources encompasses the following duties:

a) Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information
b) Protecting organizational information and resources from unauthorized use or disclosure
c) Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure
d) Observing authorized levels of access and utilizing only approved IT technology devices or services
e) Immediately reporting suspected incidents or weaknesses to IT Management

4. Unacceptable Use:

The following list is not intended to be exhaustive but is an attempt to provide examples for unacceptable use. Specific users may be granted exemptions from one or more of these restrictions by IT Management due to specific job responsibilities. If an exemption is granted, IT Management will assist with the process and with security considerations, as needed. Unacceptable use includes, but is not limited to, the following:

a) Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information,
b) Unauthorized use or disclosure of organization information and resources,
c) Distributing, transmitting, posting, or storing any electronic communications material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate,
d) Removing, altering, downloading, running, or installing any software on City-owned devices unless formally vetted and approved by the Technology Management,
e) Not abiding by copyright, contract, licensing, or other local, state, or federal laws, administrative regulations, and individual department policies,
f) Installation of any applications without authorization from the IT Management or City Management,
g) Use of personal thumb drives or any other removable devices on City computers without pre-authorization from Technology Management,
h) Attempting to represent the City in matters unrelated to official authorized job duties or responsibilities,
i) Connecting unapproved devices to the City's employee network,
j) Connecting City-owned technology resources to unauthorized networks,
k) Providing unauthorized third parties, including family and friends, access to the City's Technology resources, information, or facilities,
l) Tampering, disengaging, or otherwise circumventing the City's, another organization, or third-party IT security controls,
m) Users "sharing" system logins for accessing any of the City Systems or applications.

5. Technology access:

a) Local and Remote Access to the Network
    i) Access to the City's Domain must be granted by the IT Department
    ii) The following requests must be formally approved by IT Management:
        - Connection of any non-City system to the City Network
        - Usage of any non-standard remote access solutions (Logmein, TeamViewer, GotomyPC, etc)
        - Connection of ad-hoc Wi-Fi access points
        - Connection to the City Network of any device not issued by the City
        - Alteration of databases or data

b) Access to Wi-Fi Networks: The City provides an employee Wi-Fi network and a guest Wi-Fi network.
   i) Access to the employee Wi-Fi network is only to be used for City-Issued devices. The password will not be given out to anyone outside of the Technology Department and City Management.
   ii) The guest Wi-Fi network can be used for all non-City issued devices. It does not require a password.
   iii) IT Department shall:
      - Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
      - Authorize wireless access to the information system prior to allowing such connections.
      - Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

6. Individual Accountability:

Individual accountability is required when accessing all IT resources and City information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking the computer screen when away from the system, encrypting emails sent with sensitive data, and protecting user credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared. Additionally, users must ensure that no one else uses an account created for that specific user.

7. Additional Considerations:

a) All software and hardware must have approval of Technology Management prior to installation, removal, download or alteration. Only properly licensed programs will be considered for approval and must only be used in accordance with copyright laws.
b) All technology purchases will follow the IT-9 Procedures for New Technology Procurement policy listed in this document.
c) City IT team will follow the IT Support Document as it relates to internet security, password retrieval, system back-ups, installation of required servers and software, and copyright laws.
d) Passwords should ONLY be kept in the City-issued Password Manager application and should ONLY be shared utilizing the Password Manager application unless otherwise instructed by IT Management.
e) Security Consideration for electronic files:
   i) If an exemption is granted for disclosure of personal, private, sensitive, and/or confidential information:
      1) The authorized user is responsible for ensuring that all proper security measures are taken during transit and storage of the files (including encryption during transit and storing only in approved manners),
      2) The authorized user is responsible for ensuring that the recipient is authorized to receive the files,
      3) The authorized user is responsible for contacting the IT Department if they have any questions about the proper methods for storage and/or transmission of any files.

IT-4 Remote Access

I. PURPOSE

To define rules and requirements for connecting to the City's network from any host. These rules and requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of the City's resources.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users with a Technology resource that connects to the City's network. This policy applies to any and all technical implementations of remote access used to connect to the City's primary networks. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

It is the responsibility of the City's users with remote access privileges to the City's primary network to ensure that their remote access connection is given the same consideration as the on-site connection to the City. General access to the City's network is strictly limited to Authorized Users.

V. POLICY

1. Requirements:

a) Secure remote access must be strictly controlled with encryption (ex. Virtual Private Networks), strong pass phrases, and Two-Factor Authentication.
b) Authorized Users shall protect their login and password, even from coworkers, chain of command, IT members, family members and friends.
c) While using a City-owned computer to remotely connect to the primary network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
d) Use of external resources to conduct City business must be approved in advance by IT Management.
e) All hosts that are connected to City internal networks via remote access technologies must use the most up-to-date anti-virus software (Sentinel One), this includes personal computers.

2. Authorization:

a) Any employee requesting Remote access:
    i) Must first get their Department Head's written approval,
    ii) The approval should then be forwarded to Helpdesk with the Department Head copied on the message.
b) Any external user requesting Remote Access:
    i) Must email the Technology Director,
    ii) The Technology Director will work with the IT Team and Security Team to ensure that the need exists and the security requirements are being met.

IT-5 Authorized Equipment

I. PURPOSE

To outline the acceptable uses for computer equipment at the City. This policy is in place to protect both the employee and the City. Inappropriate use of computer equipment exposes the City to risks (examples include virus attacks, compromise of network systems and services, legal issues).

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

Internet/Intranet/Extranet-related systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts, internet browsing, and FTP, are the property of the City. These systems are to be used for City business purposes. Users must receive approval from the IT Department prior to using any technical equipment not issued by the IT Department. IT or City Management reserves the right to immediately remove access, disconnect, or repossess any equipment located on the City's domain and/or network. Each employee is responsible for proper handling of all equipment assigned to their use on a regular basis.

V. POLICY

The City invests time and money in technology systems to enable users to complete business tasks in a secure, easily accessible, and efficient manner. To prevent additional expenses and security issues, systems are provisioned to authorized users based on business needs. Each user shall be responsible for proper care of the City's property that has been assigned to them and shall be responsible for only utilizing authorized equipment during the process of completing City business.

1. Technology issued:

City-owned devices will be issued based on Department and Position requirements for the user. All issued equipment is to be returned upon separation of employment with the City. The IT Department utilizes MDM Software for all devices

a) Laptop equipment: if position requirement - employees will be issued a laptop, docking station, 2 monitors, charging cable, keyboard, and mouse
   i) It is the assigned employee's responsibility to know the location of all laptop equipment
   ii) If any of the issued equipment becomes damaged, lost, or stolen, the employee should notify their management immediately
   iii) In the event of failure of equipment, the employee should submit a support request via it.support@dunwoodyga.gov

b) Cell Phone – City employees only
   i) All City Department Heads, internal City of Dunwoody employees (based on position/need), Elected Officials, and Sworn Police Personnel have the option to receive AT&T FirstNet mobile devices
   ii) All mobile devices shall have WorkSpaceOne Mobile Device Management installed on them and the location services shall be always active
   iii) Users should NEVER use City-issued phones for personal business purposes
   iv) Any user that has a City-issued mobile phone, should NEVER use their personal phone for business (text, email, phone calls, etc.)

c) Hot Spots and Tablets
   i) All City Department Heads and Elected Officials have the option to receive an AT&T FirstNet Hot Spot and/or Tablet based on need.

2. Mobile Devices (include laptops, tablets, and Cell Phones)

a) Storing any City data, including email, on a mobile device that is not City-owned is strictly prohibited without approval of IT Management.

b) Storing non-City data, including external email, on a mobile device that is City-owned is strictly prohibited.

c) Loss or Theft of any mobile device containing City data must be reported immediately to the employee's Supervisor and the IT Department.

d) All mobile devices should have appropriate City Mobile Device Management (MDM) software installed on them:

   i) Automate MDM should be installed on all laptop devices

   ii) WorkSpace One MDM should be installed on all Cell Phones and Tablets

e) Users should ensure that their mobile device is locked whenever it is not in use (log out of laptops, and turn on the auto-lock feature on cell phones/tablets)

f) All mobile devices should be returned only after factory resetting the device, if the device has not been factory reset, it will be considered unreturned.

3. User Responsibility for Technology Equipment:

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the City and must be immediately returned upon request or at the time of user's separation from the organization. The City Management has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment. Additionally, the City Management has the discretion to charge the employee for damages if there is recurring issues or damage is due to negligence or malicious intent.

IT-6 Technology and Security

I. PURPOSE

To establish security and access measures to protect personnel, equipment, and provide backup resources for public safety.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

Access to the secured sections of the City will be limited to employees and/or persons who have specific authorization or approval to enter those secured sections. Due to different department compliance requirements, anyone entering secured areas of the building (including vendors), will need to follow proper authorization procedures prior to entry.

V. POLICY

1. CJIS Compliance

Anyone granting access to Police Department or Court secured areas will need to ensure CJIS Guidelines (CJIS Security Policy 5.9.1 and 5.12.1) are followed, at all times. Publicly accessible computers shall not be used to access, process, store, or transmit CJI.

2. Authorization

Authorization for access to secured areas can be granted by City Manager or Assistant City Manager whenever they deem it necessary. More commonly, access shall be authorized as follows:

a) Authorization to the Dunwoody Police Department secured areas can only be granted by the Terminal Agency Coordinator (TAC), or Police Department Command Staff (this includes access to the Police section of the Annex)

b) Authorization to the Dunwoody Municipal Court Department secured areas can only be granted by the Terminal Agency Coordinator (TAC), Municipal Court Management, or Police Department Command Staff

c) Authorization to the Dunwoody Technology secured areas can only be granted by the Technology Director, City Manager, or Assistant City Manager

d) Authorization to the Vital Records secured area can only be granted by the City Clerk

e) Authorization to the Human Resources secured area can only be granted by the Human Resources Director

f) Authorization to Evidence Secured areas can only be granted by Police Department Evidence staff or Police Command staff

g) Users with loanable cards are authorizing access to secured sections of the building, and as such, should ensure they are properly documenting every time they loan the card out and it's return, in addition to ensuring the card is only given to authorized individuals

3. Controlled Access to Secured Areas

All City users shall be issued an access card for entry into secured areas of the building. This access card also works as the employee ID for that user. The user is responsible for always knowing the location of their access card. Access to specific areas will be issued based on Department and Position requirements for the user. Annually, the IT Department will conduct audits of the access control system to ensure compliance. Additionally, there will be a 60 days "inactivity period" for unused cards to expire due to security reasons.

a) All access must be approved by the Dunwoody Police Department Terminal Agency Coordinator (TAC) in addition to other authorization to have access to the Police Department's secure areas (this includes access to the court clerk area connected to the patrol area and the police section of the Annex)
b) Police Officer access cards will NOT have picture IDs on them
c) Users with "loanable" access cards are responsible for immediately reporting any access cards that have not been returned
d) Under no circumstances should users release their access cards to others.
e) Users should report lost or stolen access cards to it.support@dunwoodyga.gov immediately so the card can be deactivated, and a new card issued.

4. Security cameras

There are security cameras located at City Hall, the Annex, Spruill Arts, and additional parks throughout the City. The cameras record data 24/7. Recordings are stored in compliance with Georgia Open Records Laws. For security purposes, there is a monitor located at the Police Department's PSR desk. Police Command Staff, Parks Management, City Management, Records, and IT Management all have access to the recordings.

a) Requests for footage should be made through:
   - The Police Department if the request is related to possible criminal activity or there is potential need for a police report.
     OR
   - The requesters Department Head to Technology Management if no police report or police involvement is needed (depending on the nature of the request, the Technology Management may request the Department Head go to Police Department first),

b) Requests to store recordings beyond Georgia Open Records Laws requirements must have a formal request made in writing and include details as to why the request is made and specific details including dates and exact description of cameras needed.

5. Security Reviews

a) **Scope:** Based upon a determination made by IT Management in accordance with the provisions of Section 5.b, the City may:
   i) Access and examine any Technology Resources and all Data (whether Data-In-Motion, Data-At-Rest, or Data-In-Use) utilizing Technology Resources in any manner whatsoever.
   ii) Monitor the City Network activities of individual computer users of Technology Resources.
   iii) Conduct a forensic analysis of Technology Resources, and the use and usage of such Resources.

b) **Determinations:** IT Management may exercise the rights of the City and take one or more of the actions described in Section 5.a to:
   i) Protect the integrity or security of Protected Information or Technology Resources,
   ii) Protect the City from incurring liability,
   iii) Reduce the risk of the deliberate or unwitting disclosure of Protected Information or security features of the City's Network that are not publicly known,
   iv) Investigate unusual or excessive activity typically associated with illegal activity or activity that may be in violation of the City Policies,
   v) Investigate credible allegations of illegal activity or violations of City policy; or
   vi) Comply with law or compulsory legal process.

c) **Methods and Techniques:** The IT Department may use such equipment, software, or methods as IT Management reasonably believes appropriate under the circumstances to conduct the activities described in Section 5.a. Such activities may be conducted by IT personnel or independent contractors and other vendors contractually retained by City Management for such purposes.

d) **No Expectation of Privacy:** Users of City Technology Resources for data storage, data transmission, or data dissemination, or for the processing of data should not expect that:

i) Such data is private and only accessible by them,

Or

ii) That such data is exempt from retrieval, monitoring or analysis under this policy. The City may take actions authorized under this policy with or without prior notice.

IT-7 Security Incident Reporting/Handling

I. PURPOSE

To ensure the protection of Criminal Justice Information (CJI), Criminal History Record Information (CHRI), Personally Identifiable Information (PII), and other sensitive data in the City's systems.

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. The following establishes an operational incident handling policy for the City that includes adequate preparation, detection, analysis, and containment, recovery, and user response activities as well as tracking, documenting, and appropriate incident reporting.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

1. Local Agency Security Officer (LASO): The LASO is an individual appointed by the Agency Head to assume ultimate responsibility for managing the security of CJIS systems within the agency. For the City of Dunwoody, the LASO is the Technology Director.
2. Information Security Officer (ISO): an individual appointed by GCIC and serves as the security point of contact to the FBI CJIS Division ISO and is responsible for establishing and maintaining information security policies, assesses threats and vulnerabilities, performs risk and control assessments, and oversees the governance of security operations.
3. Physically Secure Location: A facility, a police vehicle, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associate information systems.

V. POLICY

1. Security Incident Preparation, Prevention, and Handling:
   a) The City shall ensure the perimeter of all physically secure locations are prominently posted and separated from non-secure locations by physical controls.
   b) The City's Terminal Agency Coordinator (TAC) shall:
      i) Ensure general incident response roles and responsibilities are included as part of required security awareness training.
      ii) Maintain personnel listings with authorized access to the physically secure location.
      iii) Control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
   c) The City's LASO shall:
      i) Maintain automated mechanisms to assist in the reporting of security incidents.
      ii) Ensure proper tracking and documentation of information system security incidents on an ongoing basis.
      iii) Identify who is using approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
      iv) Identify and document how the equipment is connected to the state system.
      v) Ensure that personnel security screening procedures are being followed as stated in this Policy.

vi) Ensure the approved and appropriate security measures are in place and working as expected.

vii) Ensure advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise is utilized for all departmental approved mobile devices with access to CJI.

viii) Be able to easily identify connected users and devices of all departmentally approved devices with access to CJI.

ix) Track, log and manage every personally used device allowed to connect to the City's technology resources for secure CJI access.

x) Identify individuals who are responsible for reporting incidents within their area of responsibility.

xi) Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

xii) Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.

xiii) Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement point of contacts within their area.

xiv) Act as a single point of contact for their jurisdictional area for requesting incident response assistance. Track and document information system security incidents on an ongoing basis

xv) Maintain completed security incident reporting forms until the subsequent GCIC triennial audit or until legal action (if warranted) is complete; whichever timeframe is greater.

d) All authorized personnel of the City shall:

i) Monitor physical access to the information system to detect and respond to physical security incidents.

ii) Control physical access by authenticating visitors before authorizing escorted access to the physically secure location.

iii) Ensure all visitors to the physically secure location are escorted by authorized personnel and always monitored.

iv) Authorize and control information system-related items entering and exiting the physically secure location.

v) Securely store electronic and physical media within physically secure locations or controlled areas. The City shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.

vi) Protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

vii) Utilize local device authentication to unlock mobile devices authorized by the City for use in accessing CJI.

viii) Use caution when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, embedded objects, and email attachments or utilizing removable devices such as flash drives, CDs, etc.

ix) Be familiar with the City's disciplinary policy.

2. Security Incident Reporting - GCIC:

a) Any security incidents that may arise shall be reported immediately to the City's LASO. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

b) All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of City assets and are required to report any information security events and weaknesses as quickly as possible to the LASO.

c) Once notified the City's LASO will notify the Agency Head and GCIC. If deemed necessary, the City's LASO will:
   i) Notify GCIC to relay the preliminary details of the incident.
   ii) Investigate the reported incident and submit an incident response form to GCIC once all the information has been gathered.
   iii) Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with agency's standard operating procedure regarding evidence procedures.

3. Security Incident Reporting – Other Sensitive Data:
   a) Any security incidents that may arise shall be reported immediately to the City's LASO. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
   b) All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of City assets and are required to report any information security events and weaknesses as quickly as possible to the LASO.
   c) Once notified the City's LASO will notify City Management, the affected Department Head, and the Security Team. If deemed necessary, the City's LASO will:
      i) Notify Risk Management Team to relay the preliminary details of the incident to Cyber Insurance Claims and/or any other pertinent teams.
      ii) Investigate the reported incident and submit an incident response form to City Management and Risk Management Team once all the information has been gathered.
      iii) Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented and a Police Report obtained, if required.

4. Security Incident Reporting for Mobile Devices:
   a) Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.
   b) All employees of the agency with approved mobile device access to Sensitive Data shall be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of City assets and are required to report any information security events and weaknesses. Once notified the LASO will notify the City Management and the Risk Management Team.
   c) If deemed necessary the LASO will:
      i) Notify GCIC to relay the preliminary details of the incident.
      ii) Notify Risk Management Team to relay the preliminary details of the incident to Cyber Insurance Claims and/or any other pertinent teams.
      iii) Investigate the reported incident and submit an incident response form to GCIC, City Management, and Risk Management Teams once all the information has been gathered.
      iv) Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with agency's standard operating procedures regarding evidence procedures.
      v) Special reporting procedures for mobile devices shall apply in any of the following situations:
         1) **Loss of device control** - The device is in the physical control of a non-CJIS authorized individual, or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed.

2) **Total loss of device** - The physical location of the device is unknown, the device has been accidentally destroyed beyond the means of information retrieval (i.e., incinerated, shredded), or the device has been dropped in an area that prevents retrieval such as the ocean or a canyon.
3) **Device compromise** - This includes rooting, jail breaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions).

vi) In the event of a total loss of device, loss of control, or device compromise, the LASO will:

1) Enable mobile device locating features if the security of the device has not been compromised. (i.e., the device has been misplaced within the department or another secure location)
2) Contact the mobile device carrier and request assistance with device tracking.
3) If tracking for the mobile device is unsuccessful the agency LASO will:
   - Secure, control, or remotely erase all data on any department issued mobile device with Sensitive Information as deemed necessary.
   - Utilize remote features to “lock/kill” all device hardware.
     - Once the “lock/kill” feature has been activated, the LASO will contact the device carrier to ensure the mobile device has been successfully “locked/killed”.
     - If remote “lock/kill” feature is unavailable, a request to disable the mobile device via the network will be made to the device carrier.
4) If the device had CJI access:
   - The LASO will notify GCIC of loss and request assigned Originating Agency Identifier (ORI) to be deactivated.
   - Complete the reported incident investigation and submit an incident response form to GCIC once all the information has been gathered.
5) Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with agency’s standard operating procedure regarding evidence procedures.
6) All security incidents and/or GCIC violations will be reported in writing to the GCIC division director by the agency head, in accordance with GCIC policies and procedures. Sanctions: violation of any of the requirements in this policy by any authorized personnel may result in criminal prosecution by the state of Georgia, and/or administrative sanctions including, but not limited to, termination of employment with the agency.

IT-8 Security Awareness

I. PURPOSE

To raise awareness of information security, and to inform and highlight the responsibilities all users have regarding their information security obligations. Formal information security awareness will aid in the protection of data, personal, intellectual property, financial, or restricted and sensitive information, networked systems, and applications entrusted to and utilized the City, by providing a broad understanding of information security threats, risks and best practices. This policy specifies the City's internal information security awareness and training program to inform and assess all staff regarding their information security obligations.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience.

IV. GENERAL INFORMATION

The IT Department is responsible for the information security awareness program, training, education, and awareness communication for the City. The program will include Training and Testing to help produce an enhanced understanding and appreciation of information risks; provide information about potential threats, techniques, and consequences; give process for reporting incidents; guidance to protect information and devices at work and at home. Formal participation and review of the security awareness program is mandatory for anyone that uses an individually-issued City of Dunwoody email, at least annually.

V. POLICY

1. Training

All awareness training must fulfill the requirements for the security awareness program as listed below:

a) The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

b) IT Management requires that each user upon hire, and at least annually thereafter, successfully complete the current Security Awareness Training Mandatory course.

c) Newly hired employees are required to complete the current Security Awareness Training Mandatory course within thirty days of their start date.

d) From time to time, City employees may be required to complete additional training and/or remedial training courses or may be required to participate in remedial training exercises with members of the IT Department as part of a risk-based assessment.

e) Additional training is required for staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Finance Administration, Security Administration, Site Security and IT/Network Operations personnel, Human Resources Personnel, etc. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.

f) The IT Department will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

g) The IT Department will also send out regular, automated, Helpful Hints and Tricks, Top Weekly Scam, and additional information in the form of emails, flyers, posters, etc.

h) Failure to complete mandatory training within 30 days of the due date, may result in deactivation of the email account until training has been completed.

2. Simulated Social Engineering Exercises

The IT Department will conduct periodic simulated social engineering exercises including, but not limited to phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. These tests will be conducted at random throughout the year. In addition, the IT Department may conduct targeted exercises against specific departments or individuals based on a risk determination, at times.

IT-9 Procedures for New Technology Procurement

I. PURPOSE

To provide a consistent procedure to request, procure, install, develop procedures, and train on new technology for the City.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

The IT Department needs to be involved in all aspects of acquiring new technology (ex. assisting in writing the RFP to confirm that all requirements are thoroughly documented, confirming integration capabilities, confirming that implementation plans are complete, confirming hardware needs, and confirming security risks and/or concerns are addressed). Involving the IT Department from the beginning of the process can save a lot of time and potential issues throughout the process but especially during integration and/or migration. The Technology Department will issue an experienced project manager on all projects to ensure all aspects of the project go as smoothly as possible on the Dunwoody side.

V. POLICY

1. Requesting new Technology

New technology requests should always come from Department Heads or their designee.

a) Making a Request for a new application
   i) All new requests should be emailed to the Technology Director
   ii) The Technology Director will reach out to the requestor and begin the process that will vary dependent on the application, needs, etc.
   iii) Part of the process will include security vetting
   iv) Technology Department needs to be notified at the earliest opportunity to prevent delays

b) Making a Request for new equipment
   i) Department Head should email it.support@dunwoodyga.gov
   ii) Any equipment needing to be ordered could have delays due to supply issues, keep that in mind with the request and make it as soon as possible

IT-10 IT Escalation and After-Hours Emergencies

I. PURPOSE

To establish a written policy for consistent reporting and documentation of all IT related complaints, communications, escalations of IT support requests, and after-hours emergencies.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of Technology resources. This policy is applicable to all departments and users of IT resources and assets.

IV. GENERAL INFORMATION

1. For after-hours IT emergencies (entire system down, software outage, major event, catastrophic failures, work stoppage for multiple users, etc), call 678-382-6799, option 2
   a) If no one is reached and no callback is received within 15 minutes, call 678-382-6799, option 4 to speak to IT Management.
   b) If no callback is received within 15 minutes from 2nd message, call the Technology Director at 678-382-6781.
2. For urgent/emergent requests during business hours, users should call 678-382-6799, option 3.
3. For non-urgent requests, users should email it.support@dunwoodyga.gov.

V. POLICY

1. Password change requests

With the City's migration to cloud Office 365 and addition of Netwrix Password Expiration notifications, IT assistance for password changes should be rare. If a user does need help with a password reset, they should call 678-382-6799, option 3.

a) Netwrix will send out regular notifications when a user's password is scheduled to expire (7 days, 5 days, and final notice at 1 day)
b) Users have a City-issued password manager to assist them with keeping track of their passwords and should never store their passwords in any other format,
c) Users should reach out to IT anytime they need assistance generating a new password.

2. IT Emergencies

a) IT Emergencies are system outages, major events, catastrophic failures, workstopage issues for all active users with no work around,
b) All IT Emergencies should be reported via phone by dialing 678-382-6799, option 2 (regardless of time of day).

3. Emergent and/or Urgent issues

a) Emergent issues are any issues that are causing a work stoppage, with no work around, especially when multiple users are involved,
b) Urgent issues are any issues that are impeding work progress and/or ability to complete one's job,
c) All emergent and/or urgent issues should be reported via phone by dialing 678-382-6799, option 3 (regardless of time of day), user should leave a voicemail if no one answers or it is outside of normal business hours.

4. Non-Urgent updates, issues, and requests
   a) All non-urgent requests should be emailed to it.support@dunwoodyga.gov,
      i) Include a brief description of the issue as the subject of the email,
      ii) Be as detailed as possible in the body of the email,
      iii) Include screenshots of error messages, when applicable.
5. Communication
   a) The Technology Director, or designee, will send emails to all involved users during any outages, to include (but not limited to) notifications of scheduled outages, status updates during outages, and notifications when restoration is completed
   b) The Technology Department will send emails to all affected employees anytime a known risk has been identified
   c) The Technology Department will send out regular documentation on updates, changes, and "how tos", as well as offer technology training for new applications
6. Complaints and/or accolades
   a) The Technology Department is here to support the City users, and as such, would like to ensure that interactions are helpful and that the team is polite and courteous.
      i) Please email the Technology Director anytime there is a concern/complaint about the handling of a ticket, issue, lack of resolution, or negative interaction with anyone from the Technology Department (including Security, Engineers, Support, and GIS Staff) or to give constructive criticism,
      ii) Also, please email the Technology Director with any positive feedback so those experiences and efforts can be recognized as well.

IT-11 GIS Process

I. PURPOSE

To establish a written policy for streamlining the workflow process and contacting the GIS Department reference requests and questions.

II. AUTHORITY

City of Dunwoody Technology Department and City Management

III. SCOPE

This policy applies to all City employees, contractors, vendors, temporary staff, and any other users of utilizing GIS Resources.

IV. GENERAL INFORMATION

The City has two (2) Full-Time GIS staff members and one (1) Part-Time GIS Manager. Each of these team members has specific skill sets and job responsibilities. As such, all requests and questions regarding GIS should be routed through the GIS Helpdesk.

V. POLICY

1. GIS/Mapping queries

a) All queries about GIS data, requests for map layers, or specific GIS needs should be sent to gis.support@dunwoodyga.gov. That email will create a ticket where the GIS team can work collaboratively with the user to complete the request.

b) Any requests not submitted via gis.support@dunwoodyga.gov may be overlooked or forgotten.

USER ACKNOWLEDGMENT

As a user of a City Technology system, I acknowledge my responsibility to conform to the City of Dunwoody Technology Policy. These conditions apply to all users as listed in General Information and each IT Policy under “Scope”.

I acknowledge my responsibility to use the network only for official business except for such personal use involving negligible cost to the City and no interference with official business as may be permissible under the acceptable use policy.

I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I will follow the Password Policy as explained in IT-1 Section 4, “Passwords”.

I understand I am responsible for all actions taken under my account. I will not attempt to “hack” the network or any connected Automated Information System (AIS) or attempt to gain access to data for which I am not specifically authorized.

I understand my responsibility to appropriately protect all output generated under my account. I understand that I am required to ensure all hard copy material and electronic media is properly labeled as required by policies and regulations.

I understand my responsibility to report all AIS or network problems to the IT Team. I will NOT install, remove, or modify any hardware or software.

I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through IT Management. I also acknowledge my responsibility to have all official electronic media virus-scanned by the Technology Department before introducing it into the AIS or network.

I acknowledge my responsibility to conform to the requirements of the Account Management, Electronic Message, Acceptable Use Policy, Remote Access, and Technology Security Policies. I also acknowledge that failure to comply with these policies may constitute a security violation resulting in denial of access to the AIS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

I understand that I have no expectation of privacy in any equipment or media I use. I further understand that my use of technology is subject to system monitoring without advanced notification.

User (Print Name): _____ Date:_____

User Signature: _____

GLOSSARY

- CJIS: Criminal Justice Information Services Division is the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies
- DOJ: Department of Justice
- ELECTRONIC MESSAGE: Any communications sent electronically between individuals
- FBI: Federal Bureau of Investigations
- GCIC: Georgia Crime Information Center
- ISO: Information Security Officer is an individual appointed by GCIC and serves as the security point of contact to the FBI CJIS division and is responsible for establishing and maintaining information security policies
- LASO: Local Agency Security Officer is an individual appointed by the Police Agency Head or designee to assume ultimate responsibility for managing the security of CJIS systems within the City.
- MCT: Mobile Computer Terminal
- MFA OR 2FA: Multi-Factor Authentication or Two-Factor Authentication add additional security by requiring additional methods of authentication beyond a password to access a system or data
- MOBILE DEVICE: any portable electronic equipment that can connect to the internet
- NCIC: National Crime Information Center
- NIST: National Institute for Standards and Technology is a physical science laboratory and non-regulatory agency of the United States Department of Commerce with the goal to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology
- ORI: Originating Agency Identifier
- PHYSICALLY SECURE LOCATION: Any space or area with both physical and personnel security controls sufficient to protect CJI
- REMOTE ACCESS: the ability for an authorized user to access a computer or network from a geographical distance through a network connection
- TAC: Terminal Agency Coordinator is responsible for monitoring system use, enforcing system discipline, and assuring GCIC, NCIC, and CJIS operating procedures are followed.
- USER: City Employee, Contractor, Vendor, Temporary Staff, or any othe individual person with authorized access to City-Owned or Managed Technology Resources
- VPN: Virtual Private Network uses encryption over a public network, typically the internet, to access a private network