Information Technology

NYC DCAS
Citywide Administrative Services

User Responsibility Policy for Cyber Security Practices and the Use of City of New York Office and Technology Resources.

March 04, 2020 Version 3.0

This Policy, which has been approved by Deputy Commissioner IT, governs the limited personal use of the City of New York's ("City") office and technology resources by DCAS City employees, consultants and contractors.

I. The Policy

All users of the City of New York computers, systems and networks must comply with the User Responsibility policies contained herein.

II. General Policy Guidelines

DCAS City employees, consultants and contractors are required upon on-boarding to review DCAS User requirements for the use of technology, communication and computing systems, and networks. Existing employees and those on contract to DCAS must also read and acknowledge the responsibilities of use and behavior when using PCs, network, associated with reading and processing information for the tasks in their jobs. Persons using such systems must adhere to stringent policies and procedures which govern the use of restricted, sensitive and non-restricted information which they use in their jobs. Polices which this document has compiled are from DoITT, NYC Cyber Command and DCAS Cyber team (hereafter called and referred to as "DCAS Cyber policies".

Additionally, City employees are permitted limited personal use of the City's office and technology resources if the use is not prohibited pursuant to this or another applicable agency policy, does not interfere with or otherwise impede the City's operations or employee productivity, and involves no more than a minimal additional expense to the City. City employees may engage in the personal use of the City's office and technology resources permitted by this Policy only at times that do not conflict with the employee's official duties and responsibilities and the employee is not required to perform services for the City.

The opportunity that the City is extending to its employees to make limited personal use of the City's office and technology resources is only a privilege and may be revoked or limited at any time. This privilege does not create a right for any person to use any City property or resources for non-City purposes.

III. Official City of New York Office and Technology Resources Definitions:

1. "Office and technology resources" includes but is not limited to: information technology, personal computers and related peripheral equipment, software, library resources, telephones, mobile telephones, pagers and other wireless communications devices, facsimile machines, photocopiers, Internet connectivity and access to Internet services, and email.

2. "Information technology " means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
3. "Personal use" means activity that is conducted for purposes other than accomplishing official work-related activity. “Limited personal use” means the personal use of DCAS office technologies that does not result in any additional expense to the City and will employ only small amounts of resources such as internet bandwidth, electricity or ink, paper and printing toner. Personal use under this Policy does not include any use that is unlawful, or other applicable rules and regulations, or is specifically prohibited by this Policy or another applicable agency policy.
4. In the event an IT resource (e.g. desktop, monitor, laptop computer, iPhone, USB drive, tablet is lost or stolen, the employee must immediately report the incident to their supervisor, DCAS Cyber team by sending an email to cyberalerts@dcas.nyc.gov and the IT Helpdesk. The DCAS Cyber team, DoITT Security & Audit may contact you for further investigation and you maybe required to file a report.

IV. Unauthorized Uses of Technology Systems:

1. Any use of the City's office and technology resources that could cause congestion, delay, or disruption of service to any of the City's office and technology resources. For example, electronic greeting cards, video, sound, digital images or other large computer file attachments can degrade the performance of the entire network.
2. Any use of City-issued email addresses for subscribing to or registering for online personal accounts, including but not limited to, social media websites or applications (e.g., Facebook, Twitter, Instagram or E-Harmony), personal interest subscriptions (e.g., newsletters, online community groups, or Tumblr), or personal online sales accounts (e.g., Amazon, shopping websites or personal billing online accounts). City-issued email addresses may only be used for official, professional, City job-related websites.
3. Any use of the City's office and technology resources for activities that are inappropriate to the workplace or are prohibited by applicable law, rule, regulation or agency policy.
4. Any use of the City's office and technology resources for the creation, downloading, viewing, storage, copying, or transmission of any material that is: obscene, sexually explicit or sexually oriented; hate speech; threatening; defamatory; known to be fraudulent; or ridicules others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation unless your job requires you gather such information.
5. Any use of the City's office and technology resources for furtherance of a non-City business or non-City employment, including, without limitation, consulting for pay, sales or administration of business transactions (not including personal finances), or sale of goods or services.
6. Any use of the City's office and technology resources in the unauthorized acquisition, use, reproduction, transmission, or distribution of any information, computer software or data, including, without limitation: private or confidential information about any individual, business or other entity including, but not limited to, medical information; copyrighted, patented or trademarked material or material with otherwise legally protected intellectual property rights; proprietary data; or export controlled software or data.
7. Any unauthorized modification of the City's office and technology resources.

V. Privacy Expectations

1. City employees, consultants and contractors do not have an expectation of privacy while using any of the City's office and technology resources, whether for official or personal purposes, at any time, including while accessing the Internet or using email. Any use of the City's office and technology resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous. To the extent that employees wish that their personal activities remain private, they should not use the City's office and technology resources for such activities.
2. By using the City's office and technology resources, whether for official or other purposes, City employees consent to the monitoring and recording of any such use with or without cause, including, but not limited to, records of access to the Internet and email usage.

3. DCAS has the right to employ monitoring tools approved by agency senior management to ensure the proper use by employees of the City's office and technology resources. The DCAS Commissioner and Deputy Commissioners or their designees may access any electronic communications that are made using the City's office and technology resources.

VI. Cyber Polices for User Compliance

The following Cyber Security policies have been designed and approved to provide the employee a high level of secure operational controls for the use of DCAS IT resources.

The follow specific policies are to be followed by employees, consultants and contractors for the appropriate use of City of New York technology. The protections outlined below are written in accordance with City policies and standards, NIST guidelines and industry best practices.

Compliance with DCAS Cyber Security Awareness:
All DCAS employees are exposed to policies and standards as well as training tools which educate and enforce proper security behavior. DCAS has made these materials available to create at the office and at home a security culture based on employee awareness. This User Responsibility Policy describes the tasks necessary for an employee security awareness.

Password Policy:

- Passwords and PINs must never be shared or displayed on screen.
- Passwords must be changed when there is any indication of system or password compromise.
- Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored in a secure location to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.
- Passwords and PINs must have a minimum length of eight (8) characters with the exception of voice mail systems, and Blackberry and PDA devices issued by the City which must use a password or PIN of at least 4 alphanumeric characters.
- Passwords must be changed every ninety (90) days.

PC Use and Backup Policy for PCs and Removable Media:
Every PC authorized for use in DCAS must have files which are backed-up by a network file server. Every User has access to two network storage servers. The shared servers have features that differ between the services namely some are encrypted, and some are designed for work collaboration.

All work should be stored in one of several file share servers listed below. These file servers are backup automatically. Some drives are encrypted complying with the policy for storage of restricted or sensitive classified documents. The C: drive on your PC should be used as temporary workspace with file storage on one of several file stores as described in the User Responsibility Standard. S-UR-02

Removable Media:
Employees must use DCAS-issued removable media (i.e., flash drives, memory cards) to store non-confidential DCAS business related data for DCAS business purposes only.

Information Protection Policy:

- All users, consultants, and contractors are responsible and accountable for safeguarding information assets from unauthorized modification, disclosure, and destruction.
- Documents classified Restricted or Sensitive must be filed and stored appropriately when not in use and must be compliant with Information Classification and Management Policy S-RA-01. This policy includes encryption for documents and files at rest and in transit.
- Users must screen lock their active workstations when left unattended.
- Users must utilize passwords to protect city-issued PDA devices and voice mail systems.

Internet Use Policy:
The Internet should be used to conduct DCAS business. Although personal use of internet access is permitted, excessive personal use or using the internet to engage in any prohibited activities listed below may result in the employee's loss of internet access, disciplinary action or civil or criminal prosecution.

- E-mail and the Internet may be used for official DCAS work and limited personal use purposes only.
- Restricted or Sensitive classified material should be transmitted only with the use of encryption or compensating controls. Distribution of classified information including over the Internet must be compliant with Information Classification and Management Policy S-RA-01.
- Use of social media websites (e.g., Facebook, Instagram, YouTube, Twitter) should be limited to DCAS business. Although limited personal use of such sites is permitted, excessive personal use of social media websites is prohibited.

Email Use Policy:

- Employees must not open or download messages/attachments from non-trusted or unknown senders as they may contain viruses and/or malicious programs. Employees must utilize training provided to LOS units for phishing email avoidance.
- Employees must not transmit/forward obscene, profane, sexually explicit or offensive material or participate in any email list that provides access to illegal content.
- Sending restricted or sensitive City of NY data must not be transmitted to or received from any personal Web mail account.

Computer Use Policy:

- All employees are responsible for the appropriate use of all computer equipment under their control.
- Computer systems and all related computing equipment are the property of the City of New York and can be used for official Departmental purposes only.
- Users should have no expectation of privacy when using City computing resources.
- All content and traffic on DCAS and City networks may be monitored and reviewed by management.
- Unauthorized use of computing resources may result in disciplinary actions.

An investigation of misuse or from violations to this policy could be triggered by DCAS Cyber Security or IT helpdesk personnel.

Anti-Virus Security Policy:

- All servers, desktops and laptops connected to Citynet, including those on agency networks which are connected to Citynet, must participate in the Citywide managed anti-virus security cloud.
- Users shall be prevented from disabling the anti-virus agent installed on City provided computing resources.

Technology Resources Access Policy:

I. Wireless Access

- Wireless technology may be used to access, store, process or transmit City of New York business and connect to Citynet's infrastructure provided that it conforms to all applicable DoITT Information Security Policies including but not limited to this policy.
- Only approved services and applications may be used with wireless devices.

II. Remote Access Policy:

- Management approval is required before a user is authorized to use any City networking and computing resources.
- Accounts that permit access to Citynet must only be granted to users who possess an active remote access account.

- Users must be positively and individually identified and authenticated using Multi-factor authentication prior to being permitted access to any City networking and computing resource.
- Users have the responsibility of ensuring that all software, files and data accessed from remote locations entering the City's computing environment are properly virus scanned.

III. Mobile Computing Device Security Policy:

- All mobile computing devices and related virtual devices (hereafter referred to collectively as mobile computing devices) which access and/or store City of New York data must be configured, managed, used and discarded in accordance with this and all applicable Citywide security policies, standards and processes.
- The use of a City or personal smartphone device for Multi-factor Authentication to VPN private communications is permitted. Apple iPhone are the preferred smartphone device.

Enforcement & Privacy:
DCAS computers, related equipment, the E-mail system and the messages sent on it are the property of the City of New York. Internet Access of all media content is received and can be stored on the City's network servers and monitored on a regular basis. **Accordingly, employees should not assume an expectation of right to privacy in their use of DCAS-provided computers, related equipment, Internet Access, E-mail, and electronic communications at DCAS.** At any time and without prior notices, DCAS reserves the right to examine its computers, related equipment, E-mail, file directories, and information located on computers. In addition, users should be aware that Internet Access and other electronic communications may be subject to disclosure pursuant to the Freedom of Information Law and in the course of various legal proceedings. Violation of these Internet Use policies may result in disciplinary action.

System Security:
If a user discovers a security problem, that user should immediately report the problem to their supervisor, DCAS CISO and report the issue or concern on cyberalerts@dcas.nyc.gov.

Acknowledgment:

Every user of the City of New York computing resources will receive a copy of the DCAS Cyber Security User Responsibilities Policy.

I have read the above User Responsibility Policy and agree to abide to the terms and understand the penalties on non-conformance.

Signed by:

Date: _____

Employee Name:	Email:	Signature:
_____	_____	_____

DCAS Representative: Name:	Email:	Signature:
_____	UserResponsibility@dcas.nyc.gov _____	_____