AIRPORT COMMISSION OF FORSYTH COUNTY
SMITH REYNOLDS AIRPORT

Information Technology Policy

Adopted - March 21, 2017

This document is used as a guideline to create base policies for users that will be connected to, accessing, storing data on, or transmitting data across the computer network owned and operated by the Airport Commission of Forsyth County (ACFC) for the purposes of conducting its business. The Airport Director, or designee, will update this policy as needed and the new version will be posted on the Airport's web site or distributed to Users via email.

Definitions

"ACFC-owned" means the device is owned or leased by the ACFC and loaned to the user to perform ACFC business tasks.

"ACFC computer resources" as used in this policy, mean all ACFC-owned or ACFC-authorized network, system and computing resources, including related hardware and software resources. Examples include, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, web servers, standalone computers, desktops, laptop and notebook computers, telephones, radios, and other communication devices, all ACFC software, e-mail, data files, and other electronic content or communication. This definition is intended to be broadly applied and, when in doubt, users should assume that a resource provided by or hosted by the ACFC is an "ACFC computer resource."

"User" means all employees, independent contractors, consultants, temporary workers, interns, and other persons or entities who are authorized by ACFC to use ACFC computer resources.

"Material" is construed broadly to include all communication, messages, data, information files, documents and other content accessed, viewed, downloaded, uploaded, conveyed or otherwise created, stored or transmitted by or through ACFC computer resources.

Policy Violation

ACFC employees who violate this policy may have their access removed and may be subject to disciplinary action up to (and possibly including) termination. Other legal remedies, including criminal prosecution, may also be pursued if warranted. It is the policy of ACFC to handle infractions as follows:

1. The violation shall be reported to the User's supervisor or manager.
2. The User's supervisor should approach the violator(s) directly with the findings, ensure the User is aware of the policy, and give them the opportunity to cease and desist; or, depending on the severity, follow disciplinary procedures.

Technology Resource Usage

Access to and use of the telephone network, computer network, Internet and/or e-mail systems is provided to employees of the ACFC for the purpose of advancing the goals of the ACFC.
All data, e-mails, e-mail attachments, documents and other electronic information within the network/e-mail system are the property of the ACFC.

THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN COMPUTER NETWORK USE, INTERNET ACCESS, AND E-MAIL USE ON THE ACFC'S SYSTEMS.

The primary purpose for using the ACFC's Computer or Telephone network, Internet and e-mail connection is in advancing the business of the ACFC. Chats, instant messages, and text messages are NOT considered ACFC business records and should not be used to transact substantive ACFC business.

Acceptable use always is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals or other resources.

Use of the Internet by Airport Commission staff is permitted and encouraged where such use supports the goals and objectives of the Airport Commission. Internet access is to be used in a manner that is consistent with the Airport Commission's standards of business conduct and as part of the normal execution of an employee's job responsibility. The following guidelines regarding internet usage shall be followed by Users:

- Use of the Internet is monitored for legitimate security and network management reasons. Users may also be subject to limitations on their use of such resources.
- Users should never utilize the internet for visiting or posting on racist, obscene, hateful, or any other objectionable websites, or encourage other to do so on their behalf.
- Users should never upload, download, or transmit any commercial software or any copyrighted materials belonging to companies or third parties, unless the download is covered or permitted under a commercial agreement with said third parties.
- Users should never disclose any confidential information related to tenant information or any other materials deemed confidential by the ACFC.
- Users are prohibited from intentionally interfering with any implemented anti-virus, anti-spyware, anti-phishing, anti-pharming, firewall, or any other cybersecurity measures.
- Users must never intentionally interfere with the normal operation of the network, including the propagation of computer viruses or Trojans.
- Users should lock their workstations when they have finished their work, or at the end of their work hours.

Use of email by ACFC employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the organization. Email is to be used in a manner that is consistent with the ACFC's standards of business conduct and as part of the normal execution of an employee's job responsibility. The following guidelines regarding email should be followed at all times:

- In the event of a suspected crime, if legal authorities require email records, the ACFC will directly access staff email accounts in pursuit of evidence for the appropriately authorised legal or disciplinary investigation.
- Use of email may be subject to monitoring for legitimate security and / or network management reasons.
- The distribution of any information through the organization's network is subject to the scrutiny of the ACFC.
- The use of computing resources is subject to North Carolina law and any illegal use will be dealt with appropriately.
- Emails are considered records, and any records transmitted for the purpose of public business are public records, thus must not be destroyed.
- Emails should never be used to transmit any material that is racist, hateful, obscene, or defamatory or encourage others to do so on their behalf.
- The transmittal of commercial software or any copyrighted material belonging to parties outside of the ACFC is prohibited.
- Email composition should be done with care to avoid any notions of discrimination, harassment, or any other form of offensive language.
- ACFC staff should exercise diligence when opening emails from unidentified or untrusted senders.
- Before clicking on links in emails received from unidentified senders, users should hover their mouse pointer over the link to evaluate that the domain name is a recognized one.

Limited Personal Use

Authorized Users of the ACFC may also use the Internet and e-mail for limited personal use. This is a privilege, not a right, and may be limited or removed at any time. Users should also be mindful that the computers that are provided by the ACFC are the property of ACFC and must be treated as such. The ACFC does not accept liability for any loss or damage suffered by an employee as a result of that employee using the ACFC Internet connection for personal use.

Occasional, limited, appropriate, personal use of the computer system is permitted when the use does not:

- Interfere with the User's work performance.
- Interfere with the normal operation of the Airport.
- Interfere with any other User's work performance or have a negative impact on overall employee productivity.
- Have undue impact on the operation of the computer system.
- Cause any additional expense or load to the ACFC.
- Compromise the ACFC in any way.
- Violate any other provision of this policy, any other policy guideline, any law/regulation, or standard of the ACFC.

The use of public resources for personal gain and/or excessive private use by any User are absolutely prohibited and punishable, which may include termination and/or criminal prosecution depending upon the nature and severity of the transgression.

User Accounts and Passwords

Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User's password or account without express permission or portray oneself as another User. Users are expected to follow these guidelines when possible:

- Passwords shall remain confidential and should not be printed or given to others.
- Passwords may not contain your User name or any part of your full name.
- The password shall not be your birthday or other personal information such as address and phone number.

Local Computer Security

Please follow the guidelines below to help avoid security breaches:

- Close sensitive or confidential applications **and lock your computer when you leave your desk**.
- Do not leave portable media such as CDs or floppy disks in drives.
- Turn off your computer when you leave for extended periods.
- Never write your passwords on a sticky note or try to hide them anywhere in your office.
- Enable a password-protected screen saver.

Antivirus Protection

The ACFC network is protected from viruses with the help of firewalls, e-mail scanning software, and desktop scanning software. However, Users must follow these guidelines:

In some cases, simply reading an e-mail can spread a virus to a User's computer, and from there to many other internal and external ACFC recipients. The ACFC will take prudent measures to scan incoming e-mail and attempt to intercept viruses; however, no safeguard is foolproof. Each User is responsible for taking reasonable precautions to avoid introducing viruses into the ACFC network, including but not limited to:

- NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete and never forward spam, chain, and other junk e-mail.
- Never download files from unknown or suspicious sources.
- Always scan external drives (floppy, flash, DVD, etc.) from external or unknown sources for viruses before using it.
- Back up critical data and system configurations on a regular basis and store the data in a safe place.

Data Retention

In regards to data retention, the ACFC and Users shall follow these guidelines:

- Remote back-ups should be set to automatically back-up server data daily.
- Each system in the workgroup should be set to automatically back-up to an online storage cloud on a daily basis.
- Tenant information should be stored securely on the network drive and should not be disclosed to unauthorized personnel.
- Applications to construct structures which may obstruct the airspace protected by Title 14 of the Code of Federal Regulations (CFR) Part 77 will be destroyed after a retention period of 5 years.
- Airfield inspection checklists must be retained in the office for at least 1 year, after which they may be destroyed.
- The Airport Certification Manual is to be retained permanently, unless the certification has been revoked by the operator or Federal Aviation Administration (FAA).
- Airport Master Record files are to be retained for as long as they are not superseded.
- Soft copies of land development plans are to be retained permanently.
- Digital copies of capital and non-capital project files, including blueprints, are to be stored permanently, or until its usefulness expires.

Weather Emergencies & Protection of Computer Equipment

In the case of a weather emergency, the following steps are to be taken by each User to help protect both computer hardware and software.

- Backup current copy of important files.
- All computer equipment should be powered off. After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential electrical surges.
- Any equipment located on the floor should be moved to a higher location and away from any windows.
- Cover all equipment with plastic sheeting/bags and secure with masking tape. The purchasing of plastic bags and/or masking tape is the responsibility of the individual departments.