

AIR T, INC.

**Security Administration
IT Policies and Procedures
(Configuration Standards & User Access Management)**

Revision 1.0

Purpose and Scope:

This document defines the Security Administration Standards, Policies and Procedures for AIR T, INC. It covers security configuration and user account administration for employees, contractors and vendors.

Policy Statement:

AIR T, INC. expects that security and access data, servers, financial systems and technology infrastructure will comply with the provisions of this policy.

References:

None

Security Administration - Key Provisions

Security Configuration Standards

Standards related to configuration of security are documented in (Appendices A-C) for all applications, databases and operating systems. Any exceptions to the standards due to technology limitations are noted and adhered to.

User Account Management (UAM)

- There shall be a documented set of procedures for establishing and de-activating or removing user accounts for applications, operating systems and databases.
- Applications, databases and operating systems that process proprietary data will have individual user accounts and passwords. Generic user accounts will not be used for individual user access to applications and data in anyway.
- Contractor and other non-employees will have user accounts established for access to applications, databases or the network (OS). These accounts will be created and activated as needed, and set to expire on the contractor's contract termination date or earlier, as requested by a member of management.

Password Maintenance

- Each user account will have a unique password selected by the user.
- Contract and non-employee accounts will have limited access passwords set by an Administrator with an expiration date for length of project, from hours to days.
- Passwords for administrator and service accounts will be changed upon termination of any administrator that had access to the system administrator or service account passwords.

Internet Security

Internet security is handled by the use of software and hardware. We protect our Internet gateway, mail and network servers, desktops and laptops with Trend Micro NeatSuite, a fully integrated, centrally managed security suite designed to stop Web-based attacks, viruses, spyware, spam, and blended threats. Along with Trend Micro's InterScan Gateway Security Appliance (IGSA) for an additional layer to filter out Spam, Phishing, and better regulate the misuse of web sites by blocking known, non-work related problem sites.

User Account Management (UAM) Procedures

Account Creation

1. Windows Network Domain user account, Remote Access & Email

- The appropriate manager or member of Human Resources (HR) notifies IT of an employee new hire with complete name, position, start date, direct supervisor's name.
- IT acknowledges the request and creates the user account and email address.
- IT may contact the direct supervisor for information about access if there is a question to the access rights needed to perform their job.
- The user account and user's machine account are created in the appropriate Organizational Unit (OU).
- The user account is added to appropriate groups per their position with the company.
- The user account password is set to a password assigned by IT.
- The new user is given written and illustrated instructions in their new hire package on how to log on for the first time and request the password that they select for themselves. See Appendix D.

2. Financial Systems, Databases, and Folder access.

- IT creates the application user account with the required security group permissions needed to perform the job for the position they have been hired for.
- IT may contact the direct supervisor for information about access if there is a question to the access rights needed to perform their job.

3. Workstation configuration

- All workstations are set up consistently per the use of a Group Policy template that set a default user for the workstation. Restrictions are primarily on changes to:
 - the setup of the OS
 - installing any software or hardware

Account Terminations

4. Windows Network Domain user account, Remote Access & Email

- The appropriate manager or member of HR notifies IT of an employee termination and termination effective date.

- IT acknowledges the request and disables the user account, the user machine account and email address..
- The user account and user's machine account are moved to the appropriate Organizational Unit (OU).

5. Financial Systems, Databases, and Folder access.

- The application owner notifies IT of an employee termination and termination effective date.
- IT acknowledges the request and disables the user account.
- IT notifies the application owner of account termination.

6. Workstation configuration

- All workstations are taken after an employee is terminated and imaged to preserve files and state of machine at the time of termination. The machine is then cleaned to disassociate the terminated employee from the machine. Machine is generally reused for another user after these before mentioned processes.

Password Resets

7. System Accounts - Windows Network Domain user account & Remote Access

- A user may call or email the IT department with a need for an account reset or forgotten password. The IT department will assist the user with resetting the password to their newly selected password.
- The IT department will communicate the password reset to the user.

8. Financial Systems and Databases

- A user may call or email the IT department with a need for an account reset or forgotten password. The IT department will assist the user with resetting the password to their newly selected password.
- The IT department will communicate the password reset to the user.

COMPUTER USE POLICY

All users are required as part of their new hire process to read and sign the Computer use policy. Please see Appendix E.

Appendix A - Application Security Configuration Standards

AIR T, INC.					
Security Configuration Standards – Applications	MICROSOFT DYNAMICS HR/PR	AIR T ACCOUNTING Package	SYMIX SYTELINE	MAC II FLIGHT AND MAINTENANCE	QUICK BOOKS ENTERPRISE
Specific user and administrative accounts will be created and used for all employees, contractors, temps, and vendors. No generic accounts will be assigned to users.	YES	YES	YES	YES	YES
Passwords should be forced to be changed every 90 days	*YES	*YES	*YES	*YES	YES
Logins should timeout after 30 minutes of inactivity	*YES	*YES	*YES	*YES	YES
Passwords strength will be 8 characters and meet complexity requirements.	*YES	*YES	*YES	*YES	YES
The previous passwords cannot be re-used.	*YES	*YES	*YES	*YES	YES
System account passwords should be changed upon termination of an administrator	*YES	*YES	*YES	*YES	YES
Privileged access for non-employees or those not normally provided privileged access should have time-limited (expiring) access, based on reason and expected length of need.	*YES	*YES	*YES	*YES	YES
The Administrator account should not be used as a Service account and should be <i>renamed</i> to protect the system.	*YES	*YES	*YES	*YES	YES
Pre-assigned or temporary passwords must be aged to force the user to change the password within the first 7 days.	*YES	*YES	*YES	*YES	YES
Accounts should be locked out for a period of 15 minutes after 3 failed login attempts.	*YES	*YES	*YES	*YES	YES

*** These options will be driven by the Operating system user restrictions. All user application access accounts will expire at the same intervals as the Operating system accounts and all will be changed at the same time.**

Appendix B - Operating System Security Configuration Standards (Windows Server - Active Directory)

AIR T, INC.	Complies, or Noted Exception	
Security Configuration Standards – Windows	Windows Servers	
Specific user and administrative accounts will be created and used for all employees, contractors, temps, and vendors. No generic accounts will be assigned to users	Yes	
Passwords should be forced to be changed every 90 days	Yes	
Logins should timeout after 30 minutes of inactivity per screen timeout feature.	Yes	
Passwords strength will be 8 characters and meet complexity requirements. (no use of your own name)	Yes	
The previous passwords cannot be re-used.	Yes	
System account passwords should be changed upon termination of an administrator.	Yes	
Privileged access for non-employees or those not normally provided privileged access should have time-limited (expiring) access, based on reason and expected length of need.	Yes	
The Administrator account should not be used as a Service account and should be <i>renamed</i> to protect the system.	Yes	
Pre-assigned or temporary passwords must be aged to force the user to change the password within the first 7 days.	Yes	
Accounts should be locked out for a period of 15 minute after 3 failed login attempts.	Yes	

Appendix C - Database Management System (DBMS) Security Configuration Standards

Security Configuration Standards – DBMS	ALL DBMS SERVERS
Specific user and administrative accounts will be created and used for all employees, contractors, temps, and vendors. No generic accounts will be assigned to users (excludes application and system service accounts).	*Yes
Passwords should be forced to be changed every 90 days	*Yes
Logins should timeout after 15 minutes of inactivity	*Yes
Passwords strength will be 8 characters and meet complexity requirements.	*Yes
The previous passwords cannot be re-used.	*Yes
System account passwords should be changed upon termination of an administrator (including contractor/vendor changes)	*Yes
Privileged access for non-employees or those not normally provided privileged access should have time-limited (expiring) access, based on reason and expected length of need.	*Yes
The Administrator account should not be used as a Service account and should be <i>renamed</i> to protect the system.	*Yes
Pre-assigned or temporary passwords must be aged to force the user to change the password within the first seven days.	*Yes
Accounts should be locked out for a period of 15 minute after 3 failed login attempts.	*Yes

* These options will be driven by the Operating system user restrictions. All user application access accounts will expire at the same intervals as the Operating system accounts, and access to applications allows the access to the DBMS servers. All will be changed at the same time.

Appendix D – Establishing User ID and Password



To: Employees

From: Tammy Hawn, Director of IT

Attached you will find the instructions for using the company email through the internet.

Your user id and initial password will be as follows:

User Id – (first initial, last name up to 8 characters total)

Password – mountain

Please read through the document completely. Log in and send an email to Tammy Hawn, and James Burgess.

In that email give us the password that you would like to use going forward. The password must be at least 8 characters and not more than 14. Please treat this password as private.

Any questions or problems please call.

Tammy Hawn – ext – 6712

James Burgess - ext - 6708

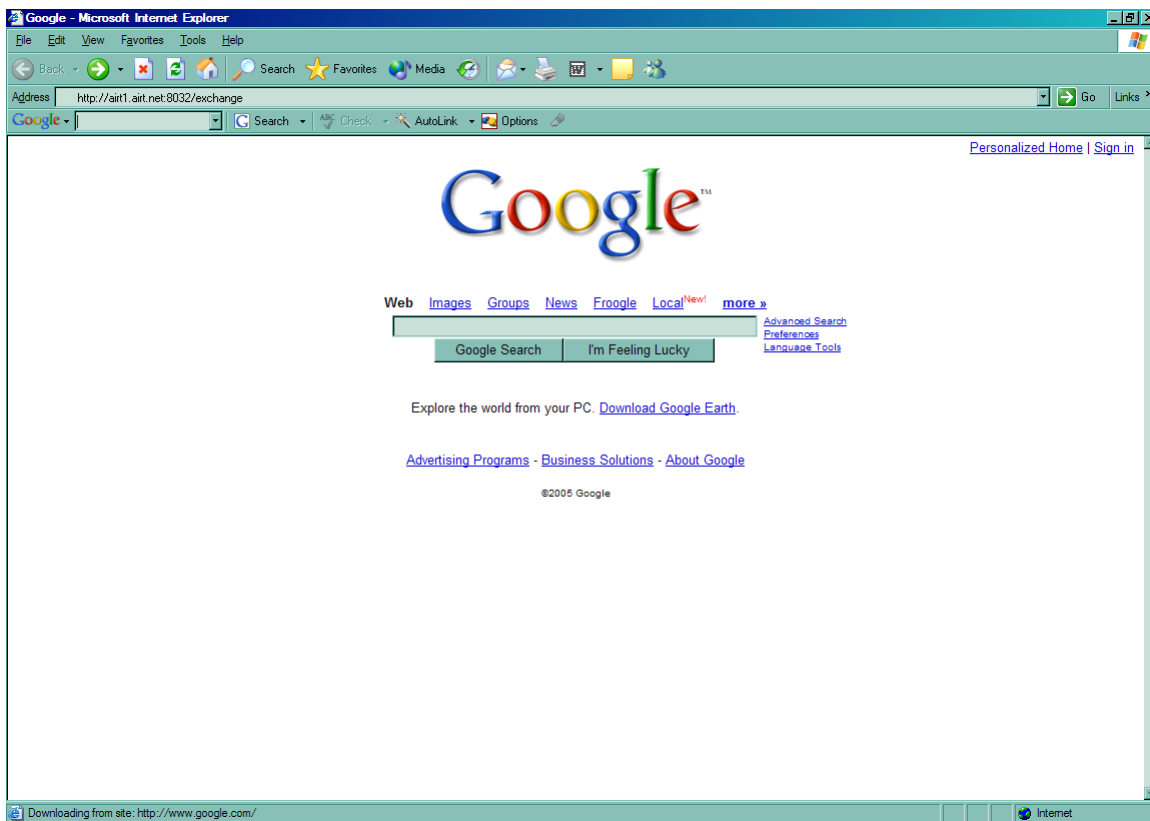


USING MICROSOFT OUTLOOK WEB ACCESS

To be able to obtain your email from any computer that has internet access, we use Microsoft Outlook Web Access.

You simply key in:

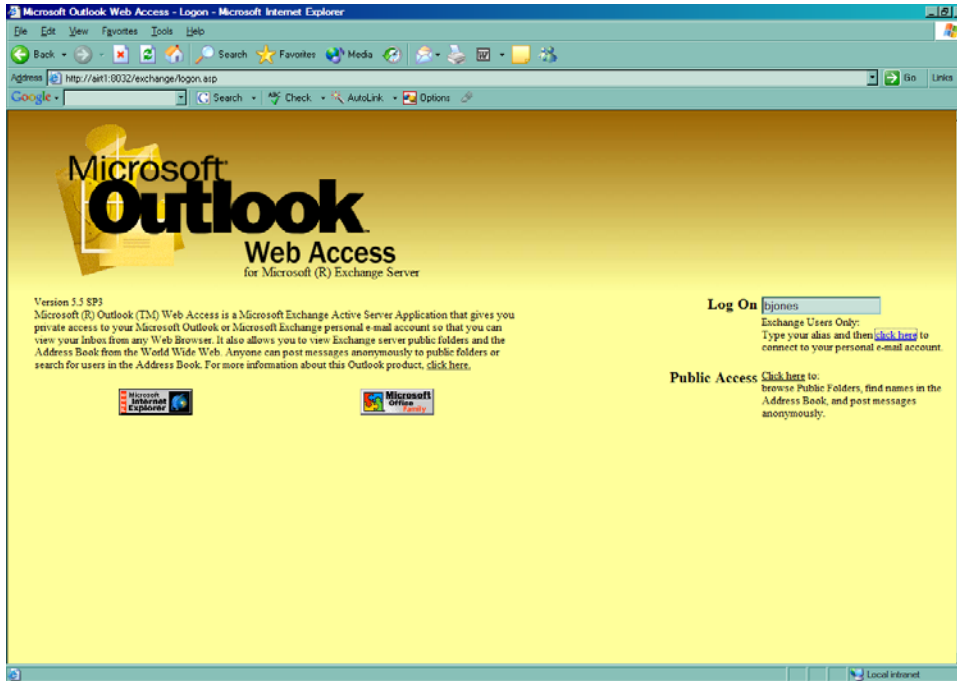
<http://airt1.airt.net:8032/exchange> on the address line of the internet browser window, as illustrated below, and press enter.



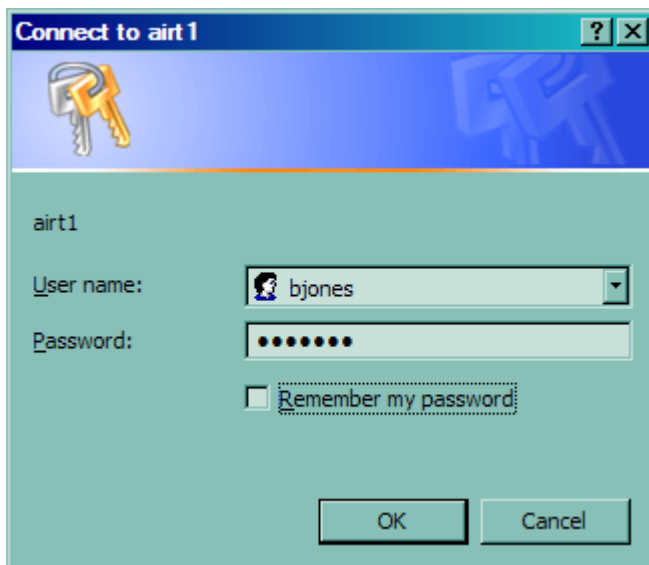
You will then see the following page where you will key in your user id. Your user id will be your first initial /last name, up to 8 characters total.

Example:

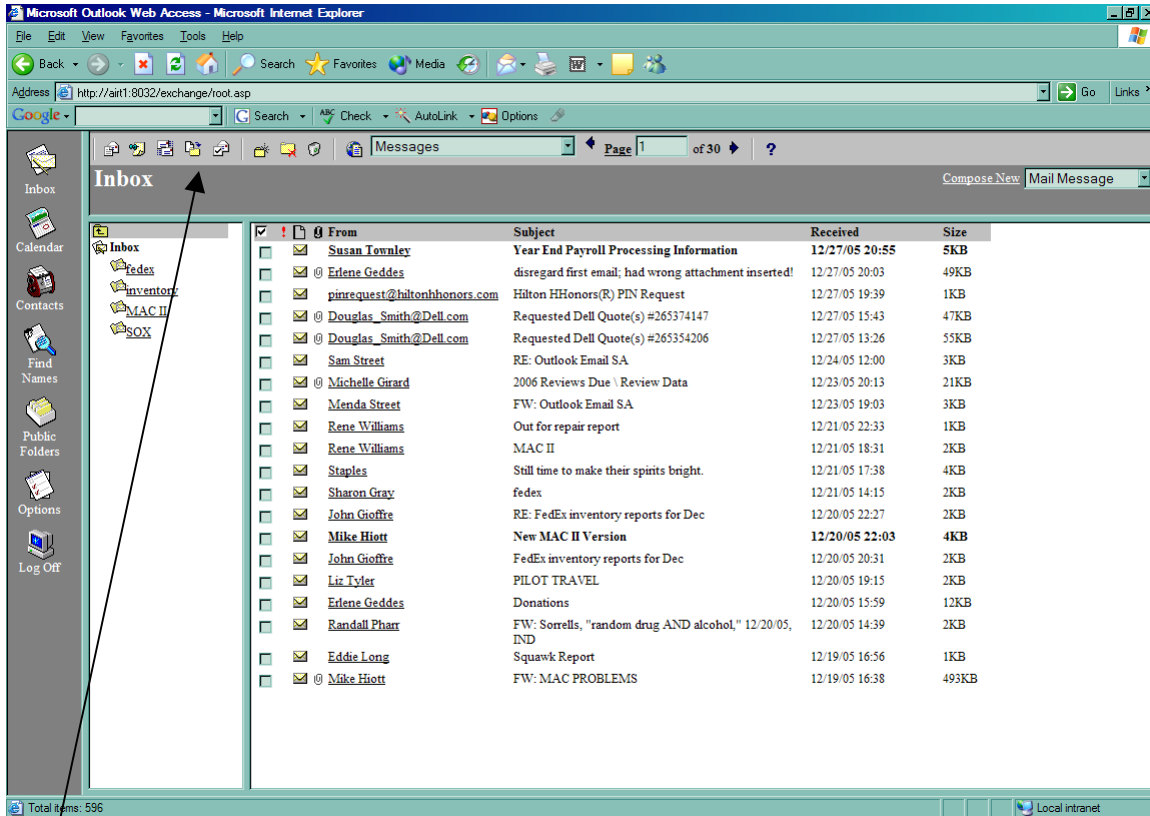
Bob Jones would be [bjones](#) ; John Underwood would be [junderwo](#)



After keying in you user id, press enter. The following box will appear. Enter your user id as above, and password, (as instructed in the preceding memo), and click OK.



A screen should appear looking similar to this one.



On the tool bar above, you can point the mouse at any of these icons and they will bring up a box with a description of what function they perform.

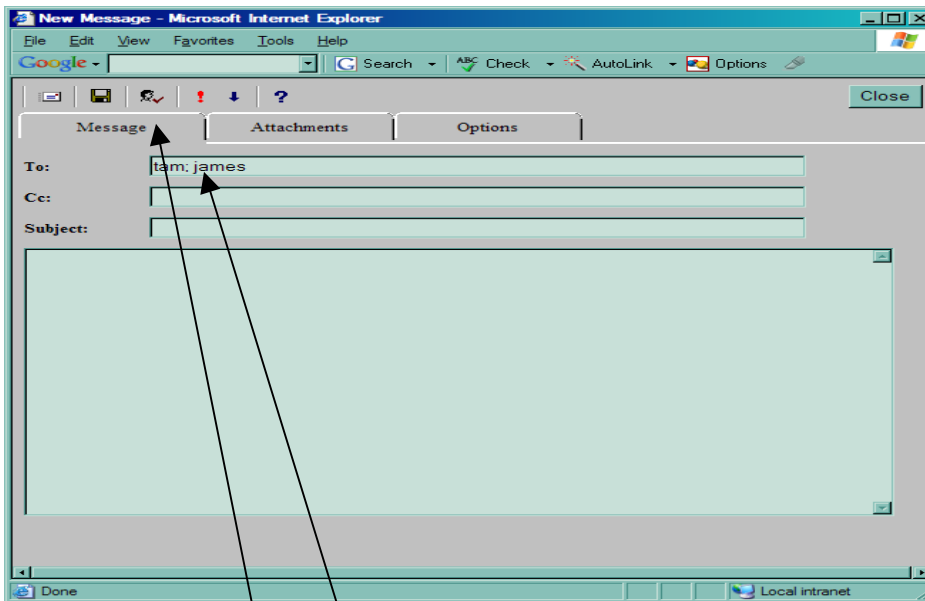
Deleting emails.

There is a check box beside each email, if you click on the check box it will insert a check mark. Then you click on the icon in the tool bar that says "delete marked items".

Creating an email.

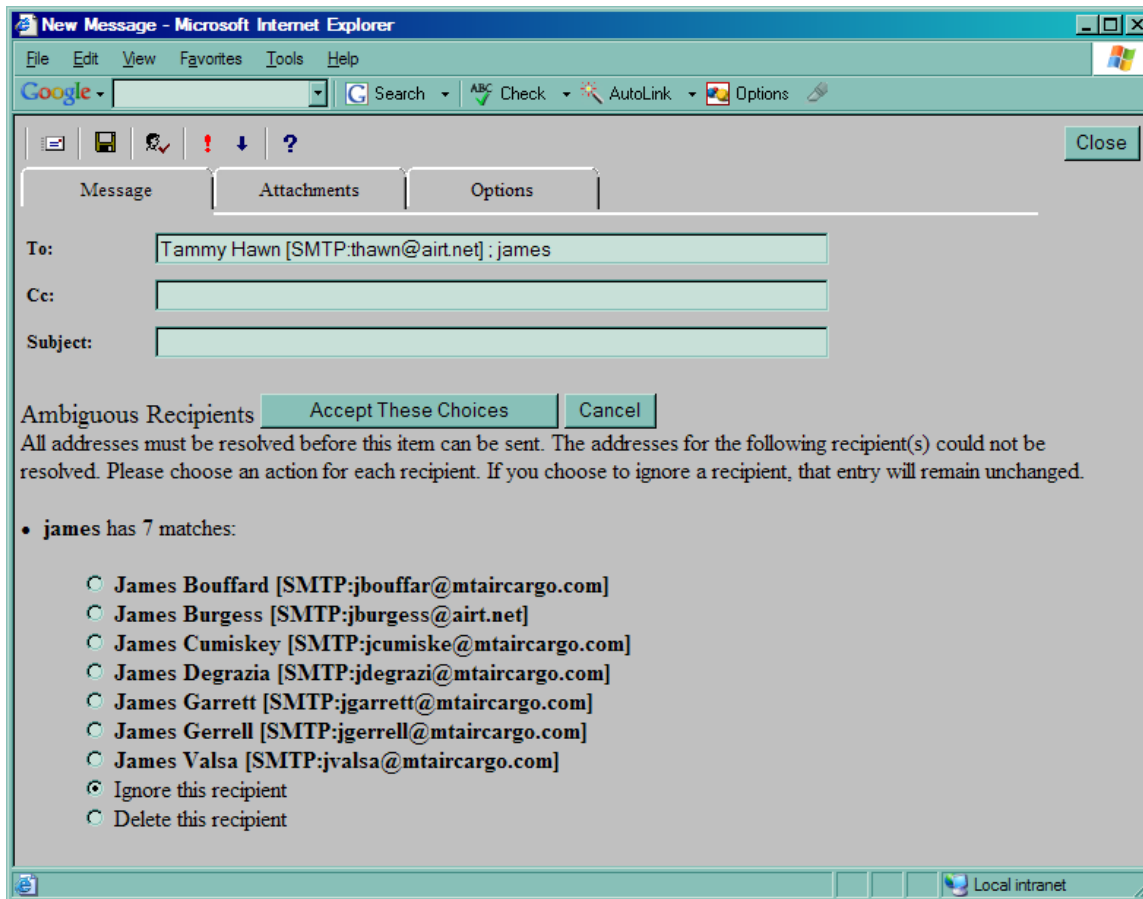
Click on the icon that says “compose new mail message”

The following screen will appear.



to use the company address book to get the email address you need, just type a portion of the first name in the “TO:” box. If you need to enter more than one name, separate them by a semi-colon (;) and a space.

For example: Let’s say we are looking for Tammy Hawn and James Burgess, and to do that we key in (tam; james) in the “TO:” box. We then click on this icon to check names. See on the following screen what happens.

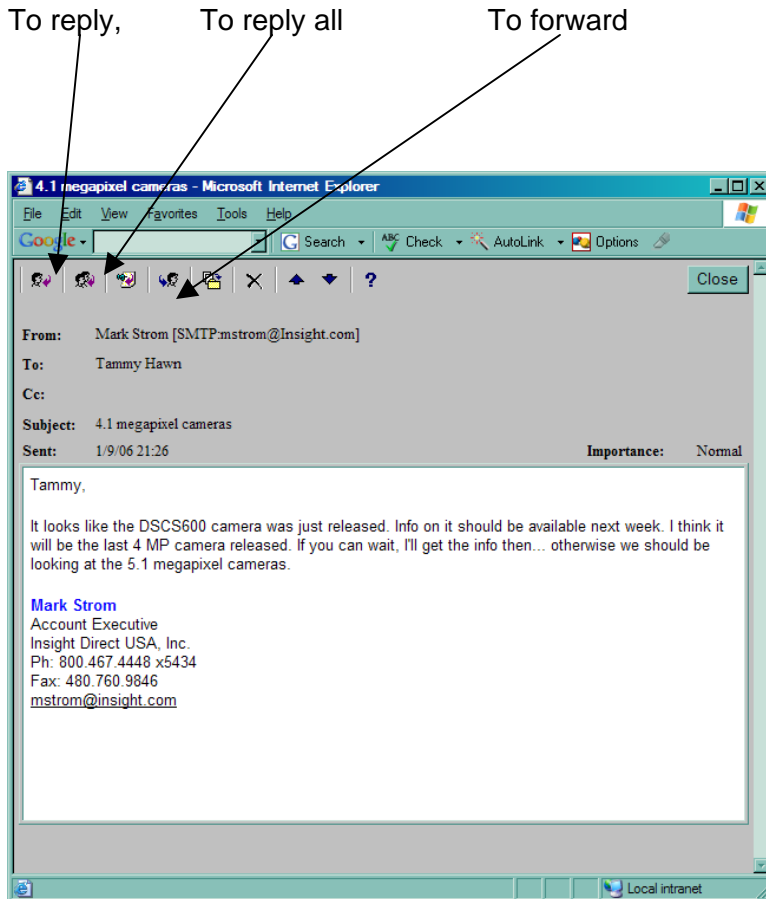


Because there is only one name that matches “tam” the email address for Tammy Hawn is automatically inserted, but because there are numerous matches for “james”, you have the option to pick which one. You click the button beside the one that you want, and click on the “Accept These Choices” button to insert the want.

Email sent to you

To open just click on the name of the person that it is sent from. The open email will look like the screen below.

Once the email is open;



Note: if you click on any of these and nothing happens, it may be that your pop-up blocker is on and will conflict with these functions. Please turn pop-up blocker off if this happens. You can disable the pop-up blocker completely or just hold down the CTRL key on your keyboard while clicking on the icon to reply or forward. This just disables the pop-up blocker temporarily in order for that function to operate.

AIR T, INC.

Computer Use Policy

PURPOSE

AIR T relies on its computer network to conduct its business. To ensure that its computer resources are used properly by its employees, independent contractors, agents, and other computer users, AIR T has created this Computer Use Policy (the "Policy").

The rules and obligations described in this Policy apply to all users (the "Users") of AIR T's computer network, wherever they may be located. Violations will be taken very seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

It is every employee's duty to use AIR T's computer resources responsibly, professionally, ethically, and lawfully.

DEFINITIONS

From time to time in this Policy, we refer to terms that require definitions:

The name *AIR T* refers to the parent company AIR T and the four subsidiary companies as follows: Mountain Air Cargo, CSA Air, Global Ground Support, and Global Aviation Services.

The term *Computer Resources* refers to AIR T's entire computer network. Specifically, Computer Resources includes, but are not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, e-mail systems, customers proprietary systems) that may be accessed directly or indirectly from AIR T's computer network.

The term *Users* refers to all employees, independent contractors, consultants, temporary workers, and other persons or entities that use AIR T's Computer Resources.

POLICY

The Computer Resources are the property of AIR T and are to be used primarily for legitimate business purposes, as it relates to the duties as employees of AIR T. Users are permitted access to the Computer Resources to assist them in performance of their jobs. Use of the computer system is a privilege that may be revoked at any time.

In using or accessing AIR T's Computer Resources, Users must comply with the following provisions.

A. NO EXPECTATION OF PRIVACY

No expectation of privacy. The computers and computer accounts given to Users are to assist them in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system hardware, software, and all data, belong to AIR T, and are to be used primarily for business purposes.

Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allowing personnel of AIR T to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that AIR T may use human or automated means to monitor use of its Computer Resources.

B. PROHIBITED ACTIVITIES

Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in AIR T's computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

Prohibited uses. Without prior written permission from AIR T management, Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political or religious material, or any other non-business use.

Waste of computer resources. Users may not deliberately perform acts that waste Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, streaming audio and video, printing multiple copies of documents, printing of large personal print jobs on printers or copiers, or otherwise creating unnecessary network traffic.

Misuse of software. Without prior written authorization from the AIR T Information Technology department, Users may **NOT** do any of the following: (1) install software on any of AIR T's workstations or servers; (2) copy software for use on their home computers; (3) provide copies of software to any independent contractors or customers of AIR T or to any third person (4) download any software from the Internet or other

online service to any of AIR T's workstations or servers; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse -engineer, disassemble, or decompile any software. Users are **not allowed** to load screen savers, desktop wallpaper, backgrounds, or sound bytes that are not furnished by AIR T as a part of the standard setup of the workstations. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

Misuse of e-mail. AIR T e-mail utilities are to be used primarily for business purposes. It is absolutely not to be used to for multiple or mass mailings that are personal and may be attempting to distribute your personal views, opinions, and/or agendas about any number of subjects. Please refrain from giving your company e-mail addresses to non-business acquaintances and please discourage all persons from sending inappropriate and non-business-related e-mail. You cannot be totally faulted for what is sent to you, but it is your responsibility to discourage it from continuing or from distributing it further. Please do not open attachments that come from unknown sources, and be aware of what you open from familiar sources.

Misuse of Internet Access. AIR T provides access to the Internet to make their employees more productive in their jobs. The Internet access is to be used primarily for business purposes. It is not the intent of AIR T to provide entertainment for break times or lunches. Use of the Internet for non-business purposes is a waste of communication bandwidth that in turn slows down the progress for those actually using it for work related reasons.

Communication of trade secrets. Unless expressly authorized by AIR T management, the sending, transmitting, or otherwise disseminating proprietary data, trade secrets, financial, or other confidential information of AIR T is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996.

C. PASSWORDS

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. AIR T owns all material stored on its computer systems.

D. SECURITY

Logging out is your best defense. If you are away from your computer for any length of time, the best protection is to log out. You will be held responsible for any actions taken on a machine during the time that you are logged in.

Accessing other user's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and e-mail.

Accessing other computers and networks. A User's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

Computer security. Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of AIR T's Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing AIR T's network without authorization and to prevent introduction and spread of viruses.

E. VIRUSES

Virus detection. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into AIR T's network. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to AIR T must be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops might contain viruses. All disks transferred from these computers to AIR T's network MUST be scanned for viruses. Diskettes are self-scanning when inserted into the machine; CDs and Flash drives are not and will need to be scanned manually by using the virus protection software on the users machine.

Accessing the Internet. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to AIR T's network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer you are using is not connected to AIR T's network.

F. ENCRYPTION SOFTWARE

Use of encryption software. Users may not install or use encryption software on any of AIR T's computers without first obtaining written permission from their supervisors. Users may not use passwords or encryption keys that are unknown to their supervisors.

Export restrictions. The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from the Information Technology Department.

G. SAFETY GUIDELINES

Protection. All computer equipment should be turned off when not in use, as with any electrical device. This applies especially at the end of the workday. This is to further safeguard the equipment from spikes or brown outs sometimes caused by storms or other power interruptions while the buildings are unoccupied.

H. MISCELLANEOUS

Amendments and revisions. This Policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

No additional rights. This Policy is not intended to, and does not grant, Users any contractual rights.

AIR T, INC.

Computer Use Policy

AGREEMENT

I have read and agree to comply with the terms of this Policy governing use of AIR T's Computer Resources. I understand that a violation of this Policy may result in disciplinary action, including possible termination, as well as civil or criminal liability.

Signature _____ Date _____

Printed name _____ Dept. _____