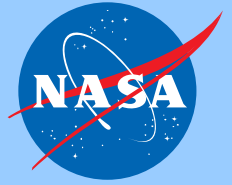


National Aeronautics and Space Administration



NASA Headquarters

New Employee IT Orientation

www.nasa.gov

Agenda

- Information Technology Overview
- Desktop Support
- IT Services
- Commonly Used HQ Wide Applications
- 358-HELP Services
- HQ Appropriate Use Policy
& IT Security Awareness Training
- Voice Mail Training
- Conclusion

Information Technology Overview

Information Technology and Communications Division

- Within the Office of Institutions and Management

<http://oim.hq.nasa.gov>

- Part of the Office of Infrastructure and Administration

<http://oim.hq.nasa.gov/oia/org.html>

- Under Headquarters Operations

http://hq.nasa.gov/OIA/itcd/documents/ITCD_orgchart.ppt

HQ Information Technology & Communications Division

- Mission:

Provide IT and communications services for NASA Headquarters employees

Use innovative solutions to increase the productivity of NASA HQ employees while achieving the highest levels of customer service

Manage and deploy cost-effective solutions into the HQ IT environment

Employee IT Responsibilities

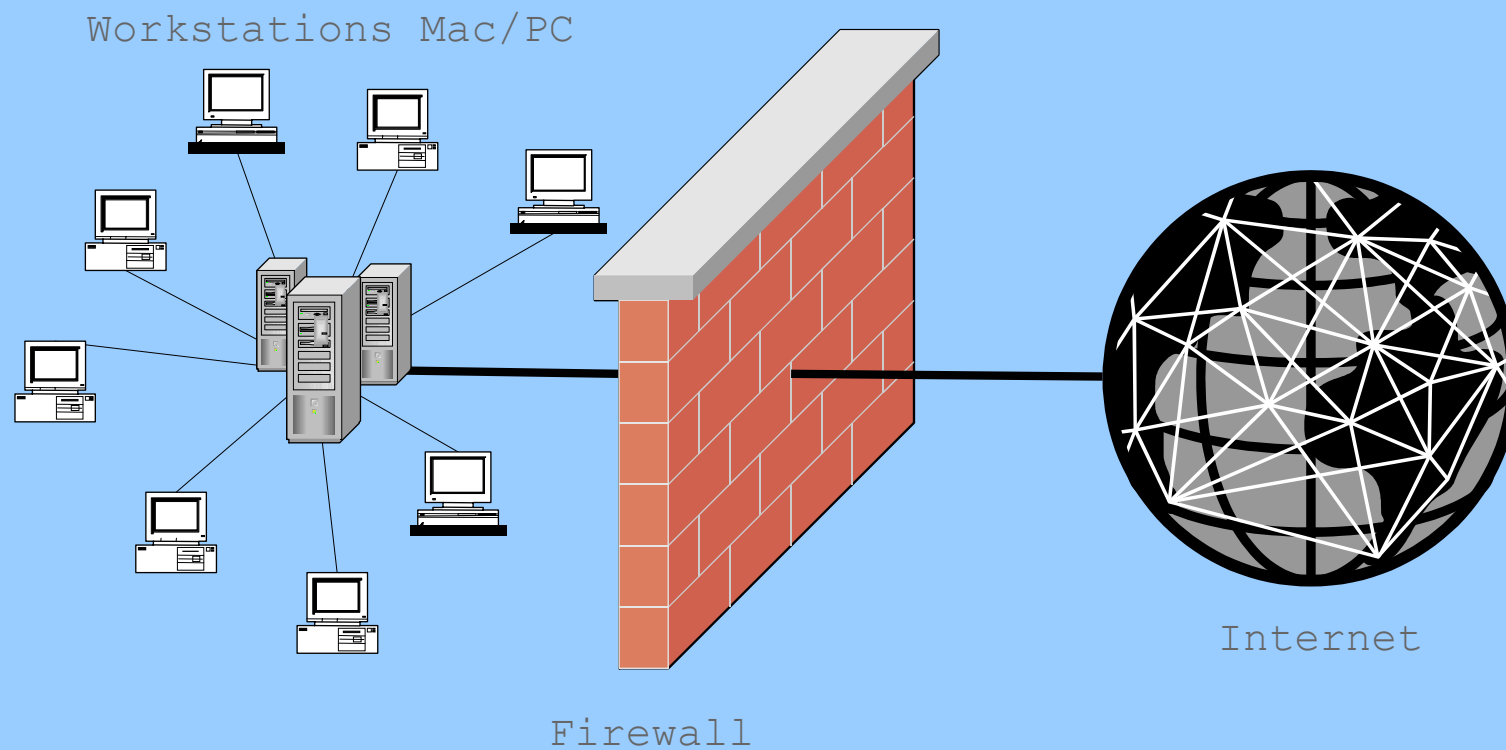
- Fill out Account Administration Forms (224, 252)
- Follow the “Appropriate Use” Policy in the performance of your duties
- Maintain your own Directory record
- Back up your hard drive (C:) *
- Obtain annual IT security training
- Call IT Help Desk at 358-HELP (4357) for all IT services, problems, and other needs
- Consult with your IT Point-of-Contact (POC) for questions and requirements that cannot be handled by the Help Desk

Communication with HQ Employees

- NASA_INC
 - Heads Up (Tuesdays & Thursdays)
 - IT Notices as needed
- Information Technology Exchanges
- Periodic Customer Advisory Committee (CAC) Meetings
- IT POCs

- *Emergency Broadcast System*

HQs IT Infrastructure Overview



Standard Desktop Hardware

- Windows XP computers
 - Desktop
 - Laptop with docking station
 - Lightweight Laptop with docking station
 - Tablets
- Apple (Macintosh OS X)
 - Desktop
 - Laptop with docking station
 - Lightweight Laptop with docking station

Standard Desktop Software

- MS Office Suite 2003 & Macintosh Office 2004
- Electronic mail and calendaring HEMI Outlook and Entourage
- Web Browsers
 - Internet Explorer for PC
 - Safari and FireFox for Macintosh
- Electronic Forms (Informed Filler)
- Acrobat Reader and Plug-Ins

Network Printers

- Printers are located within the departments for everyday work
- Color printers available throughout the building, and in the User Resource Center (URC)
- Printing facility located on C Level
 - For high-volume printing requirements
- If you have any questions call the IT Help Desk at 358-HELP (4357)
- Color printers are 18 times more expensive than b/w printers, even when printing in black and white

Storage

- Local hard drive
 - C: Drive (PC) or Macintosh HD
 - Back up your hard drive *
- Headquarters Servers
 - For Personal folders
 - » T: Drive (PC) or User ID (Mac)
 - For Group folders
 - » U: Drive (PC) or Office ID (Mac)
 - Shared drive – all users have read/write/delete access
 - » X: Drive (PC) or hq_shared (Mac)
 - For secured work group folders
 - » W: Drive (PC) or hq_groups (Mac)

Questions?

IT Services

IT Services

- Video and Teleconferencing
 - Conference Room Setup (MIC)
- Remote Access
- Guest Network
- Desktop Data Recovery (Disaster Recovery)
- Printing and Design
- Computer Training
- Web-Based Training
- User Resource Center
- Laptop Loaner Pool
- Software for Home Use
- Custom Applications
- Multimedia Support
- Telecommunications and other services
- BASO Support Services

Video and Teleconferencing

- ViTS (Video Teleconferencing System)
 - Primarily used for conferencing with other NASA centers
 - » Public facilities located on C level
 - » Other limited facilities within the departments
 - » Call 358-0146 or visit <http://intranet.hq.nasa.gov/vits/request.cfm>
- Conference Rooms (MICs) on each floor
 - On request:
 - » Computers (PCs or MACs) and projectors
 - » Voice conferencing (Need bridge number)
 - » Maintained by A/V Support <https://intranet.hq.nasa.gov/FHDS/login.cfm>
 - » Additional network connections for computers attached to the projectors
 - Always on:
 - » Network connectivity in MICs, ACR and PRC
 - » Guest Network through the Yellow Cable or wireless

Remote Access

- Connecting to HQ from Home, another Center, or while on Travel:

Traditional Dial Up:

Special set up required on accessing computer; requires SecurID token

Broadband (DSL or Cable-modem):

Other Networks

WiFi High Speed

Special set up required on accessing computer

- Accessing HQ IT Services:

Once connected to the Internet, you can access the following services:

SNA (Secure Nomadic Access)

<https://sna.hq.nasa.gov>

Requires SecurID token

VPN (Virtual Private Network)

Requires SecurID token

OWA (Outlook Web Access)

<https://webmail.nasa.gov>

Secure Nomadic Access (SNA)

- SNA allows you to access:
 - HQ Intranet Web Pages
 - NT file shares
 - OWA E-Mail and Calendaring
 - WebTADS
 - Travel Manager
- To use SNA, you need a SecurID Token
 - Issued to all new customers
 - If you do not have one, contact your IT POC to request one

SecurID Token - Resetting Your PIN

- Open a Web browser and go to <https://pollux.hq.nasa.gov/securid>
 - Enter your **UserID** in the UserName field
- For example: jdoe or rstilski (Use the 1ST initial of your 1st Name and up to the 1st seven digits of the last name)
- Look at your SecurID token and enter the current **6-digit number** displayed on the token in the PASSCODE field
 - Click **Send** (DO NOT PRESS ENTER ON YOUR KEYBOARD)
 - Create a new pin containing **4 to 8 digits**
 - Enter the new pin in both the **New PIN** and **Verify New PIN** fields
 - The pin can be all numbers, all letters, or a combination of numbers and letters. No special characters are permitted (i.e. * ! # @ % \$ & ^ ?).
 - Click **Send**
 - Your PIN has been successfully set
 - The next screen is the verification screen
 - Enter your **Username** and your newly created **pin** plus the **6-digits** appearing on your token
 - NOTE: Always wait for the next set of 6-digit numbers to change before entering
 - Click **Send**
 - You should get a message stating that if you have reached this page you have successfully initialized your pin. Your token is ready to be used.

NASA HQ Guest Network

- Wired and Wireless access

Wired access is available in most conference rooms

Look for the yellow network cable labeled "NASA Headquarters Guest Network"

Wireless access is available on all floors of the NASA Headquarters building

General office areas and conference rooms, the Library, Auditorium, and Columbia Café

- Guest Network provides basic Web, VPN, and E-mail access
- Printing is allowed to select printers inside the NASA Headquarters building

Accessing the Guest Network

- You must obtain a user name and password and authenticate using a Web browser to use the Guest Network
- You may obtain a user name and password from the following locations:
 - At the Security Desk in the West Lobby where visitors badges are obtained
 - From each organizations' IT POC
 - From the User Resource Center (URC) located in CX42
 - By having your sponsor obtain them at <http://wireless.hq.nasa.gov/> to obtain credentials and instructions

Desktop Data Recovery

- Data backup occurs nightly
 - All applications must be closed
 - Your computer must be restarted prior to leaving for the day and connected to the NASA network
 - You should not log in
 - Laptop users should leave their computers on and docked at least once per week if they desire backup services
- Initial backup up for all data in selected locations*
- Subsequent backups are incremental
- Disaster recovery service; not intended for recovery of individual “lost” files

Folders Included in Data Backup

- **Windows XP computers:**

- Local PST file (e-mail file containing stored messages and attachments)

- My Documents

- Browser bookmarks

- Desktop items

- **Macintosh computers:**

- Entourage e-mail file (local email file storage, messages and attachments)

- Contents of Documents folder

- Desktop items

- Browser bookmarks

- Keychains

- Preferences

Printing and Design

- Web Site Design
- Exhibit Designs
- Document Publishing
- Duplication

Hours - Monday through Friday, 8:00 a.m to 4:30 p.m. EST (excluding weekends and Holidays)

Location - Room CL78

Telephone - 202-358-0630

Visit <http://pd.hq.nasa.gov>

Computer Training Center

- Types of classes

 - Lunch and Learns

 - Workshops

 - Instructor-led Classes

 - Deskside (1-on-1)

- Examples of training

 - Microsoft Office Suite

 - Outlook / Entourage

 - HATS

Hours - Monday through Friday, 8:30 a.m. to 4:30 p.m. EST (excluding weekends and Holidays)

Location - Suite 3Q53

Telephone - 202-358-1111

Visit <http://ctc.hq.nasa.gov>

Web Based Training

- Attend classes online 24/7 from any location with Internet connectivity
- Some classes are instructor-led at specified dates and times
- Register once to access any classes any time
- For questions, or to register, contact the CTC:

ctc@hq.nasa.gov

358-1111

<http://ctc.hq.nasa.gov>

User Resource Center (URC)

URC personnel provide:

Walk-in technical support and services (e.g., word processing; printing; scanning; creation of graphics; CD copying; color printing; and dial-in and web access).

Hours - Monday through Friday, 7:30 a.m to 5:00 p.m. EST (excluding weekends and Holidays)

Location - Room CX42

Telephone - 202-358-1700

Laptop Loaner Pool

- Laptop Loaner Pool

Laptop loaner requests are processed via a call to the IT Help Desk at 358-HELP (4357)

Available for check-out in 4 business hours

Standard loan of up to 2 weeks

Laptop loaners are configured with the standard HQ software

Above core software can be installed if it has been purchased for your seat and licensing permits

Full size and light weight PCs and full size Macs

Also available:

- » Travel Printers and Zip Drives
- » International wireless PDAs
- » Cingular wireless cards for laptops

Handheld Devices

- Personal Digital Assistants (PDAs)

Without Wireless

With Wireless

» Data Only

» Data and Phone

See your IT POC or the Laptop Loaner Pool for information about specific models

Software For Home Use

- Available software for home use is Microsoft Office for PC and Mac, Web browser & plug-ins, Outlook 2003 for PC or Entourage for Mac, and anti-virus
- Call the IT Help Desk at 358-HELP (4357) to open a ticket requesting software
- Customer called when software is ready, usually next day, for pickup Monday-Friday, 9:00 a.m to 12:00 noon EST.

Custom Applications

- Client-server, web-based, and mainframe applications supported
- Contact your IT POC if you want to investigate a custom application.

Multimedia Support

- HQ web site design, development and maintenance
- Video digitizing for web access
- Web broadcasts to the Agency and public
- Interactive CD-ROM and DVD development

Telecommunications

- Telephones
- Voice mail
- Pagers
- Phone credit card
- Cell phones
- Handheld devices

BASO Support Services

The **B**usiness and **A**ministrative **S**ystem **O**ffice (**BASO**) provides customer support (e.g., Training, Support Line, Website) for the following IEM and eGovernment systems at NASA:

SAP R/3

Business Warehouse (BW)

Travel Manager

WebTADS

Competency Management System (CMS)

Bankcard

Workforce Integrated Management System (WIMS)

BASO Support Services

The BASO maintains the following resources for customer support:

- BASO Support Center:

Support line can be reached at 202-358-IEMP (4367)

Go-to computer stations for desk-side assistance are available in HQ Room 4R40

Available Monday-Friday 8:00am-4:30pm

- BASO Website (<http://baso.hq.nas.gov>)

Contains information for IEM applications including Job Aids, FAQs, online training courses, and links to access the systems

- Customer Training

Customers can view and sign up for all BASO instructor-led training classes via SATERN

<https://satern.nasa.gov>

Questions?

Commonly Used Headquarters Wide Applications

Commonly Used HQs Wide Applications

- Travel Authorizations and Vouchers (Travel Manager)
- Time Cards (WebTADS)
- Directory Lookup (X.500)
- Email & Calendaring (Outlook / Entourage)
- IT&CD Work Management System (IWMS)

Travel Manager

- Travel Manager is an automated, Web-based application for requesting and approving Travel Authorizations and Travel Vouchers
- A **NASA Form 1700 IEMP System Access Request** must be completed and submitted
- For additional information or Travel Manager training, contact the Business and Administrative Systems Office (BASO) at 358-IEMP (4367), via email at ifmptravel@hq.nasa.gov or visit the webpage at <http://travel.hq.nasa.gov>. BASO business hours are Monday through Friday, 8:30am to 4:30pm.

WebTADS

- WebTADS is NASA HQs time and labor collection system
- WebTADS is a web-based application that simplifies the recording of your labor and leave hours for payroll processing
- For More information call 358-IEMP

Web-based training for all HQ employees, approvers, and POCs is available at <http://webtads.hq.nasa.gov/training.htm>

X.500 Directory Services

- NASA Agency-wide directory
- Record must include full legal name from your official personnel records (i.e.)
Patrick J. Jones (official)

Patrick, Pat, Pjones, PJ, etc. (aliases)

Users are responsible for keeping information current

» To change X.500, send E-mail: Update@hq.nasa.gov with correct information

- Web site for searching:
<http://www.hq.nasa.gov/hq/x500/x500.html>

Global Address List (GAL)

- Contains name and email addresses for everyone at NASA
- Centers that are not on HEMI/NOMAD appear with a globe icon, indicating an “Internet” email address
- Easily identify someone’s Center, Org Code, and employment status
- Find other contact information if available (phone numbers, office locations, job title, etc.)
- Public distribution list groups (DL-HQ-XXXX or DL-XXXX) and Public conference rooms (CR-HQ-XXXX) are available in one location

Outlook 2003 or Entourage 2004

- Headquarters calendaring and scheduling application
 - Schedule meetings at HQ and send email invitation to non-HQ guests
 - Set-up reminders
 - View others' calendars through sharing or delegates
- Training available
 - » Call **358-1111** for assistance

SPAM Firewall

- All incoming e-mail passes through the SPAM Firewall before entering NASA Headquarters e-mail systems
- Based on policy settings, the SPAM Firewall:
 - allows the email to pass through
 - deletes the email
 - or quarantines the e-mail
- Incoming mail with any of the following characteristics is deleted:
 - contains a known virus
 - contains file attachments with known Microsoft-OS executable file extensions
 - is sent from an Internet domain whose sole intent is known to be the generation of unsolicited junk e-mail

SPAM Firewall Cont'd

- Incoming mail that has a high probability of being unsolicited junk mail is quarantined:
 - This prevents mail from cluttering up your e-mail in-box or handheld device
 - You will receive regular e-mail notifications about your e-mail being held in the quarantine, and will be able to retrieve or delete these messages yourself
- You can “train” the SPAM Firewall when it makes a mistake
 - specify Internet addresses or domain names that should always be able to send you mail (“whitelist”)
 - or addresses or domains that should never be able to send you mail (“blacklist”)

Junk Mail Folder

- It is almost impossible to stop ALL SPAM
- Should a piece of SPAM pass through the SPAM Firewall and arrive in your Outlook/Entourage inbox, you can use the built in SPAM filters in Outlook and Entourage to “train” these programs to further reduce the amount of SPAM you receive
- Outlook/Entourage SPAM filters can be trained to stop almost 99.9% of all SPAM
 - Tools, Options, Preferences, Junk E-Mail... in Outlook
 - Tools, Junk E-Mail Protection... in Entourage
- Set the level of protection you want:
 - None (NOT recommended), turns off Junk mail filtering
 - Low, catches the most obvious Junk mail
 - High, catches most junk mail, but may also trap legitimate messages
 - Safe Lists Only/Exclusive, only allows messages from people/domains you designate as safe, or from your Address Book/Contacts; all other mail goes directly to the Junk Mail folder

Junk Mail Folder Cont'd

You can “train” this SPAM filter in Outlook and Entourage when it makes a mistake

Outlook:

- » In the Junk Mail Folder....right-click...Mark as Not Junk
- » In Inbox, right-click.... Add Sender to Blocked Senders List

Entourage:

- » In the Junk Mail Folder, select the message(s), click on Message, Mark as Not Junk
- » In the Inbox, select the message(s), click on Message, Mark as Junk

Types of Calendars

Personal-business

Individuals' personal-business schedule

- Resource (Functional)

Conference Room

Activities Calendar

Calendar Management – Personal Calendars

- Personal-business Calendar

Normally the true (account) owner

Frequently SHARED with others

- » Normally a peer relationship
(e.g., Co-workers sharing job responsibilities)

May be DELEGATED to another user(s)

- » Normally a support relationship
(e.g., Executive and Administrative Assistant)
- » Delegate acts on behalf of the true owner

Calendar Management – Conference Room Calendars

- Resource Calendar – Conference Room
(Normally not a logon account)

Owner is Conference Room Administrator(s)

Conference Room is normally “invited” to meetings as a Resource

Permissions:

- » Default = Author for public conference rooms
- » Default = None for private conference rooms
- » Auto Accept = Yes
- » Reject on Conflict = Yes

May be SHARED (suggest Reviewer only)

Should Not be DELEGATED

Calendar Management – Activities Calendars

- Resource Calendar – Activities Calendar
(Normally not a logon account)

Owner is designated individual(s)

Typically SHARED by many

- » Reviewer (view/read only)
- » Author (view and change own)
- » Editor (view and change all)

Activities are scheduled by Owners, Authors, and Editors via the “Open a Shared Calendar” link

Should Not be DELEGATED

Calendar Idiosyncrasies – Changing A Meeting

- Changing A Meeting

Always choose Send Update

If you choose Save & Close, you will be prompted to send update

Save & Close **ONLY** updates your own calendar, not those of meeting attendees!

Calendar Idiosyncrasies – Canceling A Meeting

- Always send a cancellation notice

If you Delete without sending a cancellation, **ONLY** your own calendar will be updated, not those of meeting attendees!

Calendar Idiosyncrasies – Disappearing Meetings

- If you access your account on more than one computer (via Outlook, OWA, or Citrix) and accept a meeting on one, **do not** delete the invitation on the other(s).
- Doing so could remove the meeting from your calendar!

Calendar Idiosyncrasies – The “Sniffer”

- Always accept meeting invitations from your **Inbox**
- Outlook uses the “Sniffer” to place an invitation tentatively on your calendar until you accept.
- The Sniffer does **not** send a response to the organizer – only you can do that by clicking Accept, Tentative, or Decline.

Calendar Idiosyncrasies – Inviting Others

- If you know of another who should attend a meeting for which you are **not** the organizer

Send the organizer an email or call them to let them know

Do not forward the invitation – forwarding does **not** update the invitation for everyone!

Additional Applications

- The Check In Check Out (**CICO**) System
 - Web-based approval mechanism for NHQ 224 (System Access Request) that routes request through approval cycle
- IT&CD Work Management System (**IWMS**)
 - Web-based application designed to manage the IT Service Request (SR) process at HQ
- **PKI Entrust** for encrypting email
 - PGP for encrypting outside of NASA

IT Help Desk (Option 1 @ 358-HELP)

- Report Problems

Call **358-HELP (4357)** or (Toll free) 1-866-4NASAHQ (462-7247)

E-mail: service@hq.nasa.gov

- » Give detail of problem or request

Visit

<http://www.odin.lmit.com/hq/helpdesk.html>

- » Open ticket on-line

- » Check status of existing ticket

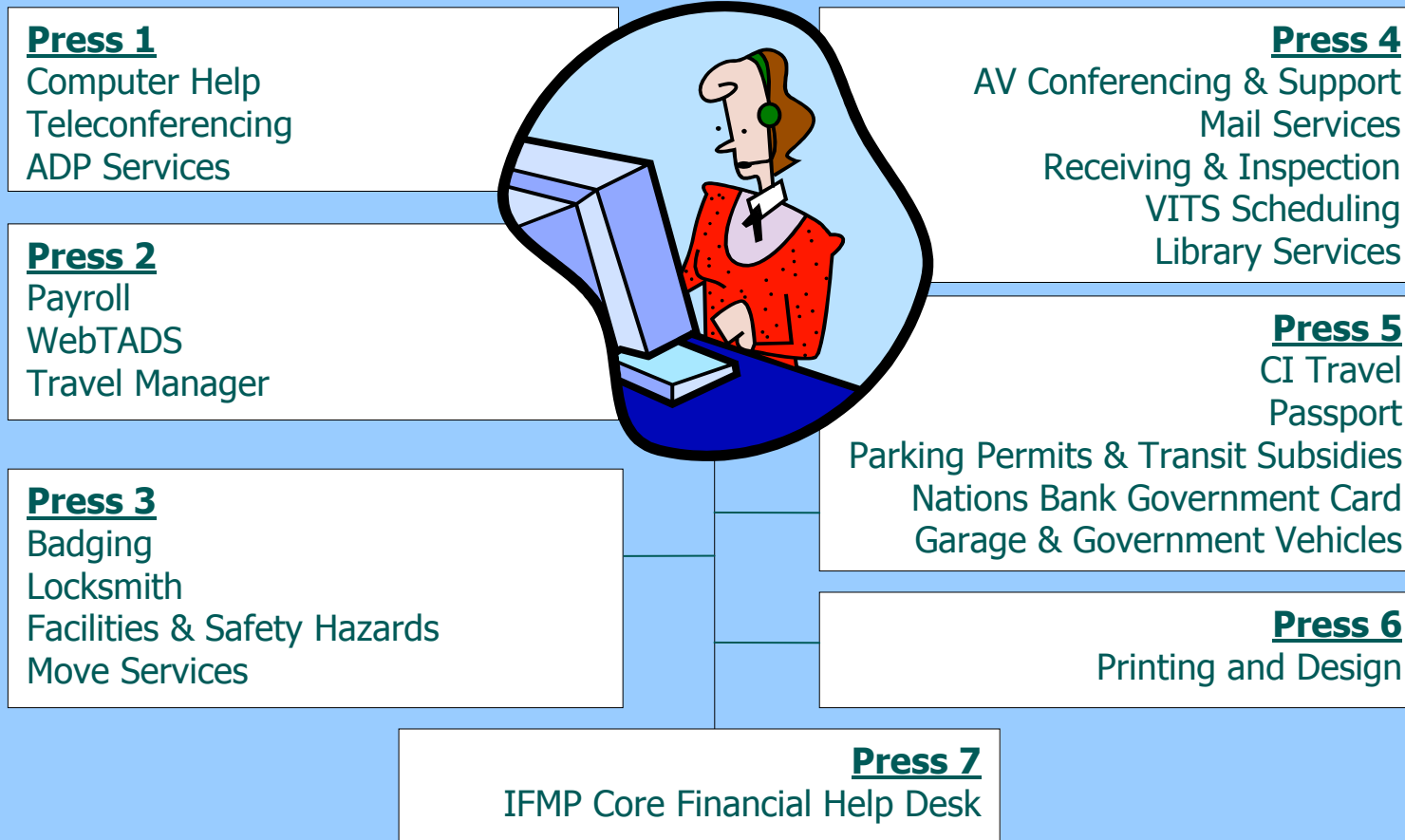
Standard Help Desk Response Times

- 8 business hours to fix problem
 - Please respond to IT Help Desk when contacted
- 30 minutes to respond to a “work stoppage”
 - 2 hours to return to service
 - Your office may be charged \$150
- Please fill out customer survey for all closed tickets
- If you do not get the support you need:
 - Ask Help Desk to escalate your requirement
 - Or call/email Customer Services Branch

After Hours Support

- NASA IT Central Help Desk is staffed 24x7x365

Phone Tree for 358-HELP



Questions?

Sensitive Information Protection Awareness Training

What and Why?

- Office of Management & Budget (OMB) memo M-06-16 (Appendix B in handout) required Agencies to take 4 actions with respect to Personally Identifiable Information (PII):
 - **Encrypt data on mobile computers**
 - Require 2-factor (token/SmartCard) authentication for remote access (Implemented at HQ)
 - Implement “time-out” limits after 30 minutes of inactivity (Implemented at HQ)
 - **Track/Log all computer-readable extracts of PII data from databases, and erase within 90 days (unless still needed).**
- Emphasis on sensitive information that is either:
 - Accessed remotely
 - Physically transported outside of Agency’s facility
- Incident reporting requirement of 1 hour from time of discovery
- NASA and the Federal Government already have applicable penalties of written reprimand to removal for 1st time offenders, 1 to 3 days suspension or removal for 2nd offenses and 7 days suspension to removal for 3rd offense. Federal consequences include fines of \$3000.00.

What is PII?

Personally Identifiable Information (PII)

- Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains.
- This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, demographic information such as age, income, and zip code, financial profiles, social security number, and credit card information.
- To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and IP address is associated with Personally Identifiable Information, then such unique information is also considered Personally Identifiable Information.
- Personally Identifiable Information does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual.

Agency Solution

- Laptops and external hard drives are required to use the following mechanisms to protect PII on the desktop and laptop:

PC: Entrust ICE

Mac: File Vault

- Entrust is the Agency tool for e-mail encryption. Mac customers will need Entrust to encrypt/un-encrypt e-mails.

Activities

- (July – Aug. 2006) - COMPLETE

Verify Entrust/File Vault encryption software installed and properly configured for HQ PII customers. Train customers to encrypt all PII data, as necessary.

Included known PII systems (per 2005 data call), as well as some HR and Budget personnel; HR and Budget personnel identified by BASO and HR

ODIN effort (the “65”), end-to-end (Forms, Installs, Education)

- (Aug. – Sept. 2006) – COMPLETE

Identify other HITSS systems that have PII data

Identified additional systems resulting in 120 more customers who need encryption software

Targeted IT Notice sent

HQ Privacy Act Manager effort: Forms, Tracking, Outreach, Training; Encryption Software Installation by ODIN

General IT Notices sent:

- » Have Customers self-identify (e.g. supervisors with access to FPPS)

HQ Appropriate Use Policy and IT Security Awareness Training

Use Of NASA IT Resources

- NASA IT Resources are for OFFICIAL BUSINESS and other less formal authorized activities.
- Limited personal use is permitted provided:
 - It does not interfere with NASA missions or operations.
 - It does not affect employee productivity.
 - It does not incur additional expense to the Government.
 - It does not violate the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635)

IT Prohibited Practices

- Any activity or exchange, which would violate federal, state, or local laws, regulations, or policies.
- Operating a private business, consulting, or sale of goods and services.

IT Prohibited Practices (cont.)

- Outside fund-raising, endorsement, lobbying, or participation in prohibited partisan political activity.
- Creation, downloading, viewing, storage, copying, or transmission of sexually explicit material or materials related to gambling, illegal weapons, terrorist activity, or controlled substances.

IT Prohibited Practices (cont.)

- Creation, copying, transmission/re-transmission of chain letters or other unauthorized mass mailings.
- Transmission of profane, obscene, abusive, offensive, or harassing statements including disparagement of others based on race, national origin, sex, sexual orientation, age, disability, religion, political beliefs, or political affiliation.

IT Prohibited Practices (cont.)

- Circumventing or disabling IT Security measures such as anti-virus software or attempting to deprive authorized users access to a resource.
- Illegal or unauthorized entry into or modification, destruction, manipulation, or denial of access to information residing on ANY information system.

IT Prohibited Practices (cont.)

- Downloading, installing, or running programs or utilities that may expose or exploit weaknesses in system security without express permission of Headquarters CIO.
- Posting NASA or other information to newsgroups, bulletin boards or other public forums without approval.

IT Prohibited Practices (cont.)

- Use of a NASA computer system in any way that might be interpreted as an attempt to influence a member of Congress regarding legislation or appropriation.
- Loading software or moves, additions, alterations, or replacement of any HQ computers, network connections cable plant, or other IT resources without express permission of Headquarters CIO.

IT Prohibited Practices (cont.)

- Unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information that includes privacy act, copyrighted, trade marked, or material with other intellectual property rights; proprietary data; or export controlled information.

A Good Rule Of Thumb

- Ask yourself:

Would I be using Government resources like this if my supervisor or the NASA administrator was looking over my shoulder?

If the answer is no, then you should refrain from the activity in your work place.

Password Procedures

- Must be at least 8 characters long.
- Must contain at least one alpha, one numeric, and one special character.
- Must not contain any form of your name, user-id, birth date, family member name, personal information, dictionary words, NASA project or Organization name, vendor product, sports team names, vehicle names, etc.
- If you must write it down – LOCK IT UP!
- Don't wait until it expires to change it.

Social Engineering

- Hackers use of lies, impersonation, tricks, bribes, threats, or blackmail to gain the information required to attack information systems.
- Don't ever provide any information over the phone or via e-mail concerning yourself or your computer unless you are absolutely certain of the identity of the solicitor.
- **NEVER PROVIDE YOUR PASSWORD TO ANYONE!**

Annual ITS Awareness Training

- All NASA employees must complete ITS Awareness Training annually
- New employee orientation DOES NOT satisfy the annual requirement
- Training is offered via the NASA SATERN Learning Management System (<https://satern.nasa.gov>) or classroom sessions at Headquarters
- See the "Training & Awareness" page at <http://www.hq.nasa.gov/security> for completion deadlines, classroom training schedules, & more information

Questions?

- Greg Kerr - HQ IT Security Manager

(202) 358-2218

Gkerr@hq.nasa.gov

- Andrew Boncek - HQ IT Technical Security Manager

(202) 358-7218

andrew.boncek-1@nasa.gov

Voice Mail

Voice Mail

- VoIP telephones
- NASA HQ Voice Messaging System
- Training available by request

Call the CTC at 358-1111 to schedule training

Conclusion

Key Points to Remember

- IT Help Desk

Call **358-HELP (4357)**

Send e-mail to: service@hq.nasa.gov

- Computer Training Center (CTC)

Call 358-1111

Send an e-mail to ctc@hq.nasa.gov

Visit <http://ctc.hq.nasa.gov>

Key Points to Remember

- Metrics:

Move/Add/Change requests. The contractor has 3 days after **NASA** approval to complete.

Problem Ticket. The contractor has 1 day to complete. User may declare a stop work. In this case, The contractor has 30 minutes to start work on a “Critical Uplift”. Costs \$150+ each time. Most “Critical Uplifts” require Customer Services Branch approval.

Key Points to Remember

- eCatalog

Large online catalog of hardware and software. The contractor has 10 days after **NASA** approval to complete.

- PC Mall

Online catalog – Same approval cycle as above; HQ employees may order for personal use at home and use personal credit card.

Key Points to Remember

- Do not:

- Disable software on your computer. Results in a \$150 charge each time

- Load (download) software or Windows patches:

- » Causes a serious breach of security

- » May result in \$150 charge for a restore to service

Key Points to Remember

- IT Help Desk will:

- Try to fix your problem on the first call

- May have to call you back

- May have to visit your workstation

- » With you present

- » Without you present

- If unable to help, will escalate your need to the Customer Services Branch

Internet References and Resources

- NASA HQ New Employee
<http://newemployee.hq.nasa.gov>
- NASA People
<http://nasapeople.nasa.gov>
- HQ Home Page
<http://www.hq.nasa.gov>
- Information Technology & Communications Home Page
<http://www.hq.nasa.gov/office/codec/codeci>
- IT Security Home Page
<http://www.hq.nasa.gov/hq/security.htm>

Internet References and Resources (cont.)

- Computer Training Center Home Page
<http://ctc.hq.nasa.gov>
- IT Security Training - SATERN
<https://satern.nasa.gov/elms/learner/login.jsp>
- WebTADS
<http://webtads.hq.nasa.gov/training.htm>
- Travel Manager
<http://travel.hq.nasa.gov/>

Customer Services Branch Phone Numbers

Noah Nason	358-1334
Michele O'Connell	358-1685
Elaine Bowman	358-1342
Joan Verbeck	358-1477
Lula Wright	358-1256
Jeff Anderson	358-1348
Mary Shouse	358-0625

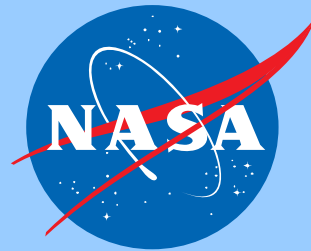
Employee IT Responsibilities

- Fill out Account Administration Forms (NHQ 252)
- Follow the “Appropriate Use” Policy in the performance of your duties.
- Obtain annual IT security training
- Maintain your own Directory record
- Back up your hard drive (C:)
- Call IT Help Desk at 358-HELP (4357) for all IT services, problems, and other needs
- Consult with the Customer Services Branch and/or your IT Point-of-Contact (POC) for questions and requirements that cannot be handled by the Help Desk

Next Steps

- Sign New User Request (NHQ 224) form
- Fill out Account Access Request (NHQ 252) form
- If needed, schedule VoIP, Outlook, or Entourage training with the CTC
358-1111
- Complete IT Orientation Survey

Thank you for your attention!



Appendix

- Data Backup

Data Backup

Why Back Up Your Data?

- Hard Drives can fail
 - Not common, particularly among HQ users
 - There have been several in recent weeks
- Protect your data by backing it up

How Often Should You Back Up Your Data?

- Back up your data as frequently as you cannot afford to do it over
 - This could be every day, or less frequently, depending upon your work needs
- In either case, you can use your Calendar or Tasks to set reminders to help you stay on top of managing your mail and data backups

What Should You Back Up?

- Aside from your mail (PST file), you should also back up:

Critical work data

Your Entrust Profile folder, if you have one

Templates you have created locally

Favorites from your Web browser

Any other files/folders you cannot afford to lose

Backing Up Your Email

- **Server Folders vs. Personal Folders**

Data in the Server folders is backed up on a regular basis

- » You have a mailbox quota of 200 Mb
- » You must manage the mail you store on the server in order to stay within your quota
- » This may require you to periodically move mail to your Personal Folders, or to an Archive file

Data in your Personal Folders is not backed up automatically

- » You must manually back it up to an appropriate location for long term, secure storage
- » The appropriate locations are detailed later in this presentation

Mailbox Folders

- Server folders are listed under your Mailbox name, usually at the top of the folder list
- Personal folders are listed under Personal Folders, usually below your server folders

Outlook Auto-archiving vs. Manual Archiving

- Auto-archiving - designed to be a local backup of data that is overwritten by new data at regular intervals

The default interval is every 14 days

The defaults can be changed by using Tools, Options in Outlook

- Should I use Auto-archive?

If you do not need to keep data older than 14 days

OR

If you rename and copy these archive files to long term, secure storage, you can take advantage of the Auto-archive feature

Auto-archiving vs. Manual Archiving, Continued

- Manual Archiving – allows you full control over what, where, and when to archive

If you need to keep data for longer periods

OR

If you want to control file naming and whether the files are overwritten, you can change the Auto-archive settings to manually archive your mail

Archiving Hints

- Regardless of whether you choose to Auto-archive or Manually Archive your mail:

Do not change the default location where the archive.pst file is created and retrieved by Outlook

» If you read the file from a network location, your archived mail could become corrupted!

Rename the file when you copy it to another storage location

OR

Label/date the media if you back up to CD-ROM or DVD/R, so that you can easily locate the file you need

Backing Up Your PST File

- Your PST file in Outlook/Entourage is where the mail in your Personal Folders is stored
- File is typically too large to fit on a standard issue flash drive (256 Mb)

You may request a larger capacity flash drive (2 or 4 Gb); see your IT POC to request one

You may burn the file to a CD-ROM or a DVD/R (if you have a DVD burner on your system)

You may save it to your User folder on the Network (T: drive)

Backing Up Your Data

- Where can you store your data?

Flash drive

CD-ROM

Hard drive

Network folders

Where Can You Store Your Data?

- Flash drives

Temporary storage used for data transfer

- CD-ROMs

Longer term storage or for data transfer

- Local Hard drive

Long term storage

- Network folders

Long term storage, data transfer between users, or for data transfer between computer systems

Flash Drives – Pros & Cons

- Pros:

- Fast, fairly high capacity (256 Mb standard; 2 – 4 Gb available), durable, and compact

- Ideal for transporting data from one physical location to another

- Nearly universal availability of USB support means they can be used almost anywhere

- Cons:

- Volatile; can sustain only a limited number of write/erase cycles before failure

- Can be damaged by misuse; typically occurs through repeated incorrect removal of device, causing loose circuit connections

CD-ROM or DVD/R Pros & Cons

- Pros:

- Higher capacity than flash drives – standard CD-ROM holds 650 or 700 Mb of data

- Single layer DVD/R can store 4.7 Gb, which is around 7 times as much as a standard CD-ROM

- Relatively easy to use

- Less volatile storage medium

- Cons:

- Must be handled and stored carefully to prevent damage to the media itself

Hard Drive – Pros & Cons

- Pros:

- Less volatile

- High capacity

- Easy to use

- Easy to organize/transfer data to and from different folders

- Cons:

- Not automatically backed up

- Not as easy to transfer data to other computer systems

Changing Your Default Save As... Locations for the Office Suite

- On a PC:

- In Excel and PowerPoint, go to Tools, Options, Save

- In Word, go to Tools, Options, File Locations

- In Access, go to Tools, Options, General

- On a Macintosh:

- In Excel, go to Excel, Preferences, General

- In PowerPoint, go to PowerPoint, Preferences, Advanced

- In Word, go to Word, Preferences, File Locations

Network Folders – Pros & Cons

- Pros:

- Least volatile due to built in redundancies

- Automatically backed up on a regular schedule

- Easy to transfer data between users or between systems

- Cons:

- Requires authentication to the network

- Your home system may require special setup or special instructions to access the network remotely

Network Folders

Level of Access	Location	Examples	Description
User-Specific	\Users (T: drive)	\Users\jdoe \Users\jhersche \Users\jsmith3	Access to files and folders restricted to the individual who owns the account
Sub-Office	Second Level of Mission Directorate/ Support Office Directory (U: drive)	Office of External Relations = \SC\ER Office of Procurement = \IM\PR Office of Human Capital Management = \IM\HCM (Note: not all Mission Directorates or Mission Support Offices are organized this way. Only those that merged two or more former codes will have this level of access)	Access to files and folders restricted to the sub-office of each Mission Directorate or Mission Support Office. Files and folders created at that level are not accessible by Mission Directorate or Mission Support staff in the other sub-offices.
Mission Directorate/ Support Office	Top-Level of Mission Directorate/ Support Office Directory	\IM (Institutions and Management) \SC (Strategic Communications) \ESMD (Exploration Systems Mission Directorate) \SMD (Science Mission Directorate)	Access available by all staff in the Mission Directorate or Mission Support Offices. Files and folders that need to be shared across the Directorate or Mission Support Office should be saved here.
Multi-Office	\hq_groups (W: drive)	\hq_groups\Budget Team \hq_groups\jennyK	Access available by request using the NHQ 224 form. Folders created here are for sharing data with specific teams created from multiple Mission Directorate and Mission Support Offices
HQ-Wide	\hq_shared (X: drive)	\hq_shared\From Bill to Jane \hq_shared\jennyK	Files and folders created here are accessible to all staff and contractors at NASA HQ. This is a temporary storage facility only. Data older than 60 days are purged to conserve data space.

Hints for Managing Your Data

- Create a task with reminder or a calendar event with reminder to archive your mail and back up your data
- Change your default Save As... location in the Office Suite to point to your User folder on the Network
- Keep a minimal amount of data locally and back it up on a regular schedule