CHESTNUT
HEALTH SYSTEMS

MIS Info Sheet for Chestnut Staff

Contacting MIS Support

Standard support hours:

8am – 5pm Monday-Friday

Submit support requests via these options…

1. Intranet: "Submit a MIS Support Request" form
2. Email to **MISSupport**
3. Phone:
   - **x3794** in the Central Region, or
   - **x1990** in the Southern Region

After-hours MIS support

For significant evening & weekend system outages or problems:

- Call: **x3718** (309-820-3718) for Central Region or **x1993** (618-512-1993) for Southern Region
  - Leave a number where you can be reached
  - If necessary, contact your ELC member or director for additional MIS phone numbers
  - Follow up with an Incident Report if needed

Non-Urgent, standard support issues: Submit a ticket or send email to MISSupport

MIS provides support for…

- Computer, email, & network issues, including VPN
- System accounts and access permissions
- Printing problems - not low toner
- Phone & voicemail issues; company cell phones
- TIER and other data systems support (e.g., fixing errors, application issues, & report writing)
- Login or Security issues
- Equipment moves
- Hardware or software requests

MIS does *not* support…

- Printer supplies, including toner (see Purchasing)
- Copiers (see Purchasing)
- Chestnut intranet & websites (see Marketing)
- Cloud-based systems (varies by department; MIS supports some but not all)
- Furniture moves (see Facilities)
- Home/personal computers & networks

When contacting MIS for support …

- Submit tickets electronically (via email or portal) whenever possible.
- Provide specific details on your request
- State when, where, and how you can be reached

Reporting IT security concerns or suspicious emails

Report any potential **security** incident or concern:

1. Send **email** to: **MISSecurity**

   or
2. **Call** the MIS phone numbers noted above (especially if the matter appears urgent)

Security Officer, **Jeff Koski** at jkoski@chestnut.org

User IDs – for YOUR use only

User IDs must *NOT* be shared.

DO NOT share your account(s) to let someone else use your computer, browse the web, or any other computing activity.

DO NOT share your badge/keycard.

Appropriate use policies

All Chestnut staff members are responsible for following appropriate use policies regarding all computing and communications systems. By company policy, Chestnut systems can monitor and record computing usage. *No staff member should have any expectation of privacy as related to his/her Internet, email, or computing system usage of any kind.*

Refer to **PP 800-840** of the Personnel Policy Handbook

See link in HR section of Intranet

System inactivity timeouts

These automatically take effect within these periods. You must then start new sessions or unlock existing sessions.

- Screensaver inactivity lockout – **10 minutes**
- VPN session ends – **12 hours**
- **TIER: *unsaved data is lost after inactivity…***
  - TIER system timeout – 25 minutes
  - TIER Remote timeout – 30 minutes

Also - see other side (rev. November 2020, jk)

Examples of IT Security incidents to report

Email **MISSecurity** or call the numbers above if you:

- Receive a phishing email or suspect a social engineering attempt
- Open a possibly infected email link or attachment
- Notice your computer is acting strangely
- Receive an anti-virus alert or other odd system alert
- Suspect someone else has accessed your account
- Have concerns that PHI has been accessed, sent, or handled in an insecure manner
- Find passwords posted in a place where others can see them, or observe staff sharing computers or otherwise using systems inappropriately
- See visitors or guests w/unapproved system access

Some simple strategies – to avoid privacy breaches and security mishaps

- Do NOT reuse passwords on multiple systems
- Use care with email (see below)
- Do NOT disclose PHI on social media
- Always keep track of your company devices and lock them when unattended
- Double check fax numbers before sending
- Use encryption on outgoing email containing PHI
- Confirm authorization validity before releasing info
- Check that you have all paperwork before leaving an office or group room.
- Be mindful of who might be able to hear patient-related conversations

Windows / email account passwords

These password rules apply to your main user account

- Passwords must be at least 8 characters long (maximum of 14 characters)
- Passwords must not contain user ID or user's name
- Complexity requirements are enforced when passwords are created or changed. Passwords must contain characters from at least three of the following four categories:
    - English uppercase characters (A – Z)
    - English lowercase characters (a – z)
    - Numbers (0 – 9)
    - Non-alphanumeric (e.g., ! $ # % &)
- Passwords must be changed every 90 days (users are reminded before expiration)

Create your own password strategy

Examples of "good", valid passwords:

– hesaGoodGuy2 or 3Red+Wagons
– Prple9919haze or h@ppyB2me!

Remember:

- Use memory cues that work for you… *…but don't use these examples!* ☺
- Passwords are case-sensitive
- Adding caps, numbers, & punctuation helps make them longer and unique
- Do **not** reuse passwords
- Be creative!

Invalid or "poor" passwords include:

– ABCDE-123 or Jkoski5512
– Mypassword1 or 12345678

Saving data – use FILE SERVERS

For security and privacy reasons, Chestnut data must be saved to **file servers**

- * Data must ***not*** be stored on–
    - USB/Flash drives
    - C:\ (your computer's hard drive)
    - CD/DVDs or other writable media
    - Web storage sites (e.g., Box, Dropbox)

    (exceptions are allowed for special cases with management and MIS approval)*
- Backups are performed on servers only. MIS does not back up local drives (C:\).

User and group server directories

Group (departmental) directories on file servers are storage areas for department-specific data. Access to group directories requires supervisor approval.

- **G:** is a region-specific shared drive
- **F:** is used for posting clinical forms
- **W:** is a cross-regional shared drive
- **H:** or **P:** are user (individual) drives for staff-specific file storage
- Departments may have other drives

Contact your supervisor or director for info on department-specific folders and files

Email tips for effective communication

- Take time write your message. Think about what you want to say and to whom you are saying it.
- Use a professional, positive tone. Don't reply to email while you're upset. Instead, save a draft to revise later before sending.
- Respond to emails in a reasonably timely manner.
- Consider whether a phone call or face-to-face meeting may be more appropriate, especially for sensitive, confidential topics and for urgent issues.
- Encrypted email should be used for external protected communications. Use approved email procedures only – See other instructions.
- Write as if your email may be shared with others or made public. All email sent can be archived, copied, or distributed to others inside and outside of Chestnut. All Chestnut emails are discoverable in any kind of legal action.
- On group emails, consider whether Reply-All is necessary or appropriate.
- Avoid "Auto-fill" addressing mistakes. Email sent to wrong recipients can result in serious breaches of PHI or other confidential information.
- Use Outlook's "Out-of-Office" feature to let others know you are away, when you will return, and who to contact in your absence.

Also - see other side (rev. November 2020, jk)