GBLS Network Security Tools

GBLS offers two tools to protect client confidentially and personal information by encrypting electronic files sent by email or carried outside the office. Below is a summary of these encryption tools and our network password policy. Please feel free to email me or the Director of Human Resources if you have any questions.

Encrypting Software: GBLS uses TrueCrypt for carrying electronic files out of the office that contains client's personal and sensitive information such as (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code. Please contact the helpdesk for TrueCrypt tutorial.

Sending Encrypted Email GBLS uses Mimecast for email spam filtering and email encryption. Using **secure:** at the beginning of an email subject line sends an encrypted email. You would only need to use this in cases where you are sending financial information in combination with a client's social security number. Contact helpdesk@gbls.org for more information. You will want to alert your colleagues that GBLS will be using encryption for email with personal information. Below is subjected text to include in the email.

Subject: Massachusetts Data Security Regulations Notice

Effective March 1, 2010, Massachusetts Data Security Regulations require businesses to take certain steps to protect the confidentiality of personal information of a Massachusetts resident. Personal Information means a Massachusetts resident's name in combination with social security number, bank account number, credit card number, driver license or state-issued identification card number. Compliance with the Massachusetts regulations will require, among other safeguards, encryption of all e-mails sent across public networks that contain Personal Information. You will receive an e-mail message from our service provider, Perimeter, informing you that you have an encrypted message. The first time that you receive notification you will be provided information on how to access a secure website and how to set up an account. In order to read an encrypted e-mail, you will need to access the secure website and enter your password.

If you have any questions regarding accessing encrypted e-mails from GBLS, please contact our IT helpdesk via e-mail (helpdesk@gbls.org).

GBLS Network Security

Computer Passwords

Passwords expire every 6 months and must meet the following criteria:

- Be a minimum of 8 characters in length
- Not include your name
- Contain a combination of upper (A, B, C...) and lower case letters (a, b, c)
- Contain at least one (1) numeric (1,2,3) or special character (&, !, @)

Consider choosing an easy to remember phrase that includes the elements above - they are much easier to remember. Please contact the helpdesk if you would like a mini-training on selecting passwords.

Locking Screen Savers

After 15 idle minutes your computer screen saver will come on and require that you enter your network password to return to your desktop.

Policy Reminders

Please remember that it is a **violation of GBLS policy to share your password with anyone including other staff,** students or volunteers.

Please remember that it is now GBLS policy that you do not use personal email accounts (Gmail, Hotmail etc.) for GBLS-related work.

Spam - Quarantine Messages

You will receive a quarantine message of emails blocked by the Mimecast system. Quarantine messages are sent each day by "Postmaster". If there are no emails requiring your review you will not receive a Quarantine message.

For each blocked email item you will have 3 options.

- **Permit**: Allows all future messages from this sender and delivers the message. This option should be selected only for known and trusted senders!
- **Block**: Blocks all future messages from this sender (does not deliver the message).
- **Release**: Delivers this particular message from the sender (messages from this sender may be blocked in the future).

Logging In to Mimecast

You will be able to log into Mimecast at any time to review your quarantine list and perform the same actions noted above. The Mimecast login link is below. Please add this link to your web browser (Internet Explorer, Mozilla) for future reference.

https://webmail-us.mimecast.com/

Your login is your GBLS email address (i.e. dbrownstein@gbls.org) and your password is the same as your login password at GBLS. The Mimecast password will automatically remain in sync with your office password when you change your GBLS password.