Data Security Directives

Data Security Directives shall be issued from time to time by the Data Security Committee to provide clarification of this policy (Data Security) or to supplement this policy (Data Security) through a more detailed procedure or specification or through action plans or timetables to aid in the implementation of specific security measures.

Directives

Computer System Security Requirement, Encryption

Password Directive

Computer System Security Requirement, Encryption

Encryption technology and algorithms must be used to protect Massachusetts PI data as defined by M.G.L. 93H and 201 CMR 17.00. Specifically, members of the University community must ensure that Massachusetts PI data as defined by the law is encrypted when (a) it is transiting a public network or a wireless network where it could be intercepted, or (b) it is stored on a portable device where it could be acquired by the theft of the entire portable device. Encryption technology and algorithms must be approved by the Director of Computer Security. Questions on this requirement can be addressed by contacting security@bc.edu.

- Massachusetts PI data transiting a public network must be encrypted by (1) using the TLS/SSL protocol, (2) using a University VPN, (3) using the SSH protocol, (4) encrypting the data in a file prior to transmission using PGP, DDPE, AES, or a similarly strong cipher, or (5) using another protocol in special cases, which can only be done with written permission from the Director of Computer Security.
  - Boston College servers providing TLS/SSL, SSH, or VPN encryption to meet this requirement must not offer a "debug" option to users during normal operation. This option, which may have a different title with different protocols, turns off encryption. “Debug” is only to be available in controlled test environments for troubleshooting.
- Massachusetts PI data transiting a wireless network must be encrypted using the same five choices listed in the previous bullet, unless the wireless network is internal to Boston College and is tagged as "secure" by the University.
- Users that store Massachusetts PI on a laptop must use the "PGP Whole Disk Encryption" or "Dell DDPE" software offered through Information Technology.
Services if possible, or, if using an alternative protection mechanism, must obtain written permission from the Director of Computer Security.

- Users are not permitted to store Massachusetts PI, including email messages containing Massachusetts PI, on a so-called "smartphones" or other ultra-portable computing devices unless (a) the device being used provides encryption and (b) the provided encryption is activated, irrespective of whether said device is owned by the University or by an individual.

Password Directive

Passwords should be changed periodically to ensure that any third party access to a user’s credentials is cut off. Passwords can be obtained by unauthorized parties through a variety of subversive techniques, including software that records keystrokes, “phishing,” hacking, and even simple observation. A user whose credentials are stolen in such a fashion may not even realize that the credentials are compromised. As such, it is best practice to change passwords periodically. On the other hand, BC recognizes that too-frequent password changes are inconvenient, create a support burden, and bring their own problems, such as users recording new passwords in lieu of memorization. Within this directive, **Boston College credentials** means the username and password combination used to log into the Agora Portal and other common BC services. These are sometimes referred to as the “main” or “LDAP” credentials.

- The password of each user’s Boston College credentials must be changed at least yearly.

- User passwords associated with other Boston College systems that are not linked directly to the Boston College credentials must also be changed at least yearly.

- User accounts that have administrative-level access to any shared, multi-user system or application must be changed at least every six months.

- Under no circumstances should Boston College credentials be re-used as credentials on any system, application, web site, etc. not owned by the university or contracted by the university to provide some specific service(s). (e.g. do not use a BC email and BC password for a mail account outside of BC, like Gmail, Hotmail, or Yahoo; do not use BC credentials for access to financial accounts like bank, brokerage, retirement; do not use for catalog sites...)
Need Help?

If you require further information about the specifics of this directive or how it might affect you, please contact your Data Security Officer (DSO) or ITS Security at security@bc.edu.