Password, Authentication and Access Standard

Policy Type: Administrative
Responsible Office: Office of Technology Services, Information Security
Initial Policy Approved: 11/14/2016
Current Revision Approved: 01/24/2017

Standard Statement and Purpose

This standard establishes security requirements when formulating and using passwords, passphrases, or other means to access VCU information and authenticate against VCU Information Technology (IT) systems. The requirements stated within this policy are applicable to all users of IT systems that are used to generate, process, transmit, and store VCU information. **NOTE:** this may include an individual's mobile device.

Electronic access to all VCU information classified as category II or category I must be authorized by data steward or designee and protected by authentication methods as outlined in this policy.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard

All individuals who generate, access, process, transmit, and store VCU Information on work issued or personal devices.

Definitions

Administrative Access

Access to an IT system's operating system or user interface, which can allow the person to modify the behavior or settings within the IT system or the data contained in the IT system. Examples of administrative access include access to the Windows Operating System, access to shell or command line, and access to an administrative web interface for a web application. Transactional use of an IT system, such as the use of a web form to input data, is not within the scope of administrative access.

Administrative or System Level Accounts

Administrative or system level accounts are accounts used by system or application administrators to monitor and manage IT systems and / or applications. Examples of these accounts include: root, Administrator, sysadmin, application accounts, or other system or application administrator accounts.

Appliances

Within the context of this document, appliances refer to IT systems or equipment that closely integrate the hardware and software components, and are designed to provide a specific computing resource. Examples of an Appliance can include Network routers, switches, firewalls, and some computerized research equipment such as electron microscopes.

Application

Within the context of this document, an application is a software package that is designed to assist the individuals using it in accomplishing certain business tasks. An application can be both an installed software located on a computer system; and a website designed to convert certain input into specific output.

Application Account

Within the context of this document, application accounts are accounts and passwords used by an application or IT system to communicate with another IT system for the proper function of the application or IT system. These accounts are never used by human beings to login to IT systems or applications. An example of such account will be a web server account used by an application to communicate with a backend database.

Authenticate / Authentication

Authenticate is the action in which an entity verifies its identity with another entity. Examples of authentication include the use of a password to logon to an IT system, the use of certificates to establish a trust between two IT systems, and the examination of a picture ID presented by an individual.

Automatic logon

Within the context of this document, automatic logon refers to a process where the password to a system or application is stored in a computer system, and using these stored credentials, a process can allow the individual accessing a system or application to automatically logon to such system and application and without being prompted to enter the password or authentication credentials.

CFR Title 21 Part 11 (FDA) covered Information

Data or information that are received from the U.S. Food and Drug Administration (FDA), usually through sponsored research projects or protocols are covered under this regulation.

Console Access

Within the context of this document, console access refers to an individual's authentication to and subsequent use of a computer system while the individual is physically present at the location of the computer system and directly interacting with the computer system. An example of console access is the access of an individual's office computer using the keyboard and mice attached to the computer.

Controlled Unclassified Information (CUI)

Information from federal agencies that requires the protection delineated under the NIST SP800-171 standards. These information typically are received as a part of a research project, and are required through the Federal Acquisition Regulation clauses. Although dubious at the moment, the U.S. National Archive is made the authoritative source for the definition of CUI, and the list of potentially covered information can be found at the National Archive CUI Registry: https://www.archives.gov/cui/registry/category-list.html

Criminal Justice Information

Information regulated under the FBI Criminal Justice Information Services (CJIS) Security Standard, this includes any information provided by the FBI CJIS necessary for law enforcement and civil agencies to perform their missions including, but are not limited to biometric, identity history, biographic, property, and case / incident history data. Like many other regulations, CJIS Security Standards also carries a transient property, where whether an organization receives the data directly or indirectly from a third party, such data will be regulated by the security standards. VCUPD and certain research projects may have access or store these data.

Data Categorization

Within the context of this document, data categorization is the process for individuals to review and classify the content of the data and information in their possession. The categorization process will follow the data classification standards provided by the University and data will be classified into three different categories in accordance to its sensitivity.

Data Custodian

A data custodian is an individual or organization in physical or logical possession of data for Data Stewards. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls. The Data Custodians are directly responsible for the physical and logical security of the systems and data that are under their control.

Data Steward

A Data Steward is a University director or equivalent employee who oversees the capture, maintenance and dissemination of data for a particular operation. The Data Steward is responsible to ensure data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate "business rules" and monitor data quality within the source system and/or data warehouse. The data steward is also responsible for communicating data protection requirements to the Data Custodian, defining requirements for access to the data.

Data Trustee

A Data Trustee will carry out plans and policies to implement appropriate data management practices as defined by applicable industry regulations and University policies and procedures. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, Provost and Senior Vice President of Academic Affairs, Senior Vice President of Finance and Administration or Senior Vice President of Health Sciences. Data trustees are ultimately responsible for the consistency, integrity, and security of the data under their purview.

dbGaP

Data from the database of Genotypes and Phenotypes developed and maintained by the National Center for Biotechnology Information. Data from this database is regulated under the dbGaP Security Best Practices.

Federal Information Security Management Act (FISMA)

Federal Information Security Management Act (FISMA) requires the use of the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 as a common security framework for the management of various information belonging to federal government. The framework outlines the expected security controls for information that are rated at the low, moderate, or high level, where each level requires additional controls to be implemented. This regulation can impact the research projects involving federal government data, or projects that are funded by federal government. The moderate and high level controls are a set of minimal baseline set to handle any data with medium to high sensitivity.

Handheld Mobile Devices

Within the context of this document, Handheld Mobile Devices refer to Smart Phones, Pad or Tablet devices, and Personal Digital Assistants (PDAs) that use mobile operating systems such as iOS, Android, Symbian, Windows Phone, Windows Mobile, and Blackberry OS.

Off-site remote Access

Within the context of this document, Off-site remote access refers to access to any VCU IT systems or data from non-VCU locations and / or not using official VCU networks. Examples of Off-site remote access include, but are not limited to: access from home, access from a hotel while traveling, access from a Smart Phone while using the cellular provider network.

On-site remote Access

Within the context of this document, On-site remote access refers to access to any VCU IT systems or data from VCU locations and / or VCU networks; but not directly from the location where the system is located. Examples of On-site remote access include, but are not limited to: accessing a VCU application hosted in the Computer Center from a school computer lab, remote desktop access to a server hosted in the Computer Center from an office on campus, accessing a VCU system or information from a Smart Phone while using the VCU wireless network.

Passphrase

A passphrase is an actual phrase made up of multiple words that are used by individuals, in conjunction with their user names, to access an IT system. Passphrases are typically long and complex, thus making them harder to guess and compromise by attackers. Additionally, due to the fact that they are sentences, they are easier to remember, and may not need to be written down. Examples of passphrases include: “ILuvPepperon1P1zza” and “VCURamzAllTh3Way”

Payment Card Industry Data Security Standard (PCI-DSS)

Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to alleviate vulnerabilities that put cardholder data at risk.

Second-Factor Authentication / Multi-Factor Authentication

The three factors of authentication include: “something you know”, “something you are”, and “something you have”. A password / passphrase is considered “something you know”, and can be considered as a single factor. A second factor for authentication simply means that another one of the aforementioned factors must also be used to authenticate an individual, in conjunction with the individual’s password / passphrase. Examples of second factors include, but are not limited to: Fingerprint (something you are), voice recognition (something you are), smart card / token (something you have), and cell phone (something you have)

The Cancer Genome Atlas (TCGA) Information

Data from The Cancer Genome Atlas data repository developed and maintained by the National Cancer Institute, regulated by the TCGA data use agreement, which enforces dbGaP Security Best Practices and the Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS)

VCU Information

VCU Information refers to information in paper, electronic or oral format that is collected, generated, transmitted, processed or stored by a VCU employee, consultant, contractor or other affiliate in the course of their work and is used to support the academic, research, patient care or administrative operations in VCU.

VCU owned IT systems

Unless specified otherwise by the sponsoring funding source, all IT systems, including servers, appliances, workstations, desktops, laptops, and any mobile devices, that are purchased with funding allocated to the Virginia Commonwealth University, or its employees for the purpose of education, research, and administration.

Virtual Private Network (VPN)

Virtual Private Network (VPN) is a technology that allows an individual residing outside of the University network to connect and access information and technology resources that are accessible only to individuals inside of a University network. Individuals using VPN to connect into the University are authenticated through the use of their unique IDs, and authorized to access certain resources on the internal University network that are otherwise not available to an individual on the Internet.

Contacts

VCU Technology Services (Technology Services) officially interprets this Standard. The VCU Information Security Office (Information Security Office) is responsible for obtaining approval through the appropriate governance structures. Questions about this Standard should be directed to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following section of this document delineates the authentication and password requirements in handling and storage of VCU information. Requirements for the handling and storage of such information are set at a minimum and also further defined by specific Data categories, requiring additional security measures. For the most detailed information on data categories and classification, please see the VCU Data Classification Standard.

1. **Basic Password / Passphrase requirements for IT systems**: Where possible, VCU recommends the use of a passphrase instead of the traditional password. Avoid writing down passwords and passphrases, if written passwords and passphrases are needed, the written passwords / passphrase must be physically secured, and cannot be located in a publicly accessible area. Rather than writing down passwords / passphrases, they can be stored in secure electronic password databases. Inquire with your local IT personnel or the Information Security Office.

   a. The following requirements apply to **all VCU owned IT systems**:

      i. Passwords or passphrases are required for administrative access to any VCU owned IT systems and must be changed whenever there is a change in the staff that has administrative access and whenever there is a suspicion of possible system compromise.
      ii. All default administrative passwords must be changed on all IT systems and applications prior to production system deployment.
      iii. Passwords or Passphrases used for administrative or system level accounts must be unique and not used as passwords for other accounts the administrator may have on the system.
      iv. Password or Passphrase must be at least 12 characters in length.
      v. Password or Passphrase must contain at least one uppercase character, one lower case character, and one number and / or a special character.
      vi. Must not contain the username, real name, or company name

vii. Must not be comprised of a single dictionary word (G3)

b. The following password and passphrase complexity and expiration requirement applies to **all VCU owned handheld mobile devices**:

i. Device must be protected with passwords / passcodes with at least 4 digits in length; unless reasonable biometrics or other comparable authentication is used.

ii. User access to mobile devices must be suspended for at least 30 minutes following no more than 10 consecutive failed login attempts.

iii. Passcode or other authentication protection must be enabled following no longer than 10 minutes of inactivity.

c. The following password and passphrase requirement applies to **all application accounts used by VCU owned IT systems**:

i. Password or Passphrase must:

1. be at least 16 characters in length; and
2. contains at least one uppercase character, one lower case character, and one number.

ii. Application access to IT system or database must be temporarily suspended following a defined number of unsuccessful login attempts. The criteria for this setting must be commensurate to the sensitivity of the information and IT system.

iii. Password protection is required for each unique session between the application and the database or IT system.

iv. Application accounts must be:

1. unique to the application
2. each application must use a dedicated and unique account to access other systems and databases
3. must be designated to application use only, individual administrative access to IT systems using application accounts to is prohibited

v. Application account passwords and passphrases **must not be** hard coded into the applications without encryption or another form of comparable protection.

2. **Category III Information Authentication and Access Requirements**: The following password / passphrase requirements apply to any access of Category III information.

a. Application of passcode, password or passphrase protection when accessing Category III information is at the discretion of the Data Steward or designee.

b. If used, passcodes, passwords and passphrases are expected to meet the requirements delineated in the *Basic Password / Passphrase requirements for IT systems* section; as shown above.

c. Passwords and passphrases of individuals uniquely identify each individual, and must be kept secret and cannot be shared with others. All individuals are expected to use their assigned login credentials. At no time is it permitted to use another individual's login credentials. (M1)

d. Passcodes, passwords and passphrases must not be inserted into email messages or other forms of electronic communication without encryption or alternate but comparable forms of protection. (G19)

e. Passcodes, passwords and passphrases must not be stored in a file or computer system without encryption or alternate but comparable forms of protection. (G17)

f. Passcodes, passwords and passphrases must not be stored on Internet or cloud based file storage systems without encryption or alternate but comparable form of protection. (G17)

g. Passcodes, passwords and passphrases entered onto a screen during authentication must be masked as they are entered. (G35)

3. **Category II Information Authentication and Access Requirements:** The password requirements delineated in this section are applicable to any access of information that are classified at Category II or higher. In addition to or in place of the requirements from the Category III section, affected individuals must also adhere to the following requirements.

a. Ensure Category III authentication requirements are met from the previous section (*Category III Information Authentication Requirements*)

b. In addition to authorization from the data steward or designee, network, system, and information access will only be granted following reasonable and successful authentication of individual identity. Acceptable authentication methods include one or a combination of the following:

i. Passwords and Passphrases / Passcodes for mobile devices
ii. Keycards
iii. Keys
iv. Fingerprint (Hand Scanner)
v. Retina / Iris Scanners (G1)

c. Passwords and passphrases must be unique, and the previous ten passwords or passphrases for accounts must be kept in history, so that they are not re-used. (G3)

d. Excluding application accounts, passwords / passphrases for all personnel with access to information must be changed every 365 days at a minimum. (G6)

e. Individual identity must be verified before the issuance and modification of authentication credentials. Verification must consist of a combination of something only the individual knows, something only the individual has, or an in person identification with ID. (M17)

f. Excluding usernames, rather than re-issuing existing authentication credentials, new replacement temporary credential must be issued to individuals who forgot their passwords, passphrases, and other authentication credentials. (M17)

g. Temporary passwords and passphrases must be used when granting initial access to data or system to an individual, where the individual must change the temporary password immediately after the first logon. (M17)

h. All temporary passwords and passphrases must be unique to an individual. (M17)

i. The identity of an individual must be verified before a temporary password is issued to the individual, and the individual must acknowledge the reception of the password.

j. All systems that transmit, process, and store Category II Information must enable automatic account lock following no more than 10 failed logon attempts within 5 minutes. All failed access attempts must be logged, including source, destination, date, time, and username information. (H17)

k. Unless explicitly re-enabled by an administrator, all accounts that have been automatically locked out must remain locked out for 30 minutes at a minimum. Continued access attempts must be logged with source, destination, date, time, and username. (H21)

l. All user accounts must be disabled after 365 days of inactivity. Disablement must be documented and electronic information related to disabled accounts must be maintained in accordance with VCU Record Retention Policy and applicable schedules. (G15)

m. Units using shared or group accounts must establish procedures for the secure re-issuance of the shared or group account credentials following the separation of an individual with access to the account. The procedures must address the following:

    i. Periodic review and removal of individuals with no need to access the account
    ii. Process to reset password / passphrase / passcode
    iii. Secured storage of the shared credentials
    iv. Secure dissemination of the credentials to all individuals assigned to the account

(N29)

4. **Category I Information Authentication and Access Requirements:** The password requirements delineated in this section are applicable to any access of data that are classified at Category I or higher. In addition to or in place of the requirements from the Category II section, affected individuals must also adhere to the following requirements.

   a. Ensure Category III and Category II authentication requirements are met from the previous sections (*Category III Information Authentication Requirements and Category information authentication requirements*)

   b. Access to Category I information must be authorized by data steward or designee and authenticated by a unique credentials assigned to each individual. Use of shared or group accounts to access this information is prohibited. (G25)

   c. System and / or security administrators must be immediately notified of all automatic account lockout events for accounts used to access Category I information. Acceptable notification methods include e-Mail, Short Message Service (SMS), and phone call. If failed logon attempts persist, the system and / or administrator must immediately inform the system owner and Information Security Office for further investigation. (H23)

   d. All devices used to access or store data must automatically lock the user session after no more than 30 minutes of inactivity. All users must re-authenticate to unlock the session. (H11)

   e. Off-site remote access to Category I systems and information, other than those data of your own, must use VCU centrally managed Virtual Private Network (VPN) connections with multi-factor authentication, or other comparable multi-factor authentication methods. (J10)

   f. Off-site remote administrative access to Category I IT systems must use VCU centrally managed Virtual Private Network (VPN) connections with multi-factor authentication, or other comparable multi-factor authentication methods. (J9)

   g. Multi-factor authentication is required for On-site remote administrative access to Category I IT systems. (J11, J25)

5. **Special Requirements for Selected Regulated Information:** Aside from the requirements delineated in previous sections, the following requirements apply to access to specific data and information. All data types delineated in the section below are considered Category I data, but have specific requirements as required by applicable regulations. The following requirements

will apply in addition to, or in place of documented requirements presented above.

a. All usernames assigned to personnel with access to applicable information must be longer than six characters. *Applies to dbGap and TCGA research data* (G2)

b. Passwords and passphrases for all personnel handling applicable data must be changed every 90 days. *Applies to dbGaP and TCGA research data, PCI-DSS regulated data, and CJIS regulated data.* (G5)

c. All access to applicable information must be protected by multi-factor authentication. This requirement applies to any access to information, regardless of information or user location. *Applies to FISMA Moderate + High information, CUI, Export Controlled Information, CFR Title 21 regulated information.* (G7)

d. All user accounts for systems that transmit, process, or store applicable information must be disabled after 90 days of inactivity. Disablement must be documented and electronic information related to disabled accounts must be maintained in accordance with VCU Record Retention Policy and applicable schedules. *Applies to PCI-DSS regulated data.* (G16)

e. All systems that transmit, process, or store applicable Information must enable automatic account lock following no more than 5 consecutive failed attempts. All failed access attempts must be logged, including source, destination, date, time, and username information. *Applies to PCI-DSS regulated data and CJIS regulated data.* (H18 + H19)

f. All systems that transmit, process, or store applicable Information must enable automatic account lock following no more than 3 consecutive failed attempts. All failed access attempts must be logged, including source, destination, date, time, and username information. *Applies to FISMA Moderate + High information* (H20)

g. For systems that transmit, process, or store applicable information, all accounts that have been automatically locked out must remain locked out, until it is explicitly re-enabled by an administrator. Continued access attempts must be logged with source, destination, date, time, and username. *Applies to FISMA Moderate + High information* (H22)

h. All devices used to transmit, process, or store information must automatically lock the user session after no more than 15 minutes of inactivity. All users must re-authenticate to unlock the session. *Applies to dbGaP and TCGA research data, PCI-DSS regulated data.* (H12)

i. Ensure tamper resistance is built into authentication mechanisms to prevent credential replay and re-use attacks. *Applies to CUI and FISMA Moderate + High information.* (G36)

j. Multi-factor authentication is required for on-site console access to system used to transmit, process, or store information. *Applies to CUI and FISMA Moderate + High information.* (H58)

k. When used, non-biometric electronic signatures executed by an individual must be verified via 2 identification components, such as an identification code and a password. Continued signing of applicable information within one session must require the execution of at least one of the identification components for each signing. New sessions must require the use of at least 2 identification components. *Applies to CFR Title 21 Part 11 (FDA) information* (Q9)

l. Individual using electronic signature to authenticate and access information must certify their agreement that electronic signatures used are legally binding as physical signature before use. Certification shall be submitted to applicable regulatory agency along with physical signature, and upon request, additional certifications may be needed. *Applies to CFR Title 21 Part 11 (FDA) information.* (Q10)

6. **Request for Exception:** All requests for exception(s) to this policy are evaluated by the Information Security Office on a case-by-case basis. Exception requests should be made using the Information Security Exception Request Form. The completed exception request form is automatically emailed the Authoritative Unit Head listed in the request. After the Authoritative Unit Head approves the request, the Information Security Office will provide the secondary review and approval as appropriate. Evaluation criteria for exception include the requirement to which an exception is requested, the sensitivity of the information affected, compensating controls in place to mitigate additional risks, and business processes affected by the exception. The Information Security Office will send the exception request review decision and any additional correspondence to the requestor's and the authoritative unit head's email addresses.

Forms

1. VCU Information Security Exception Request Form

Related Documents

The VCU Information Technology Policy Framework contains VCU Information Technology policies, standards and baseline requirements, all of which must be followed in conjunction with this standard. The framework also includes information technology guidelines as recommendations and best practices. Other related documents are listed below.

1. **VCU Information Security Policy**
2. **VCU Computer and Network Resource Use Policy**
3. **VCU Data Classification Standard**
4. **ISO / IEC 27001 and 27002 Standards and Techniques**
5. **VCU Record Retention Standard**

Revision History

This policy supersedes the following archived policies:

April 19, 2007	*Password Standard*
November 30, 2009	*Information Security Standard – Section 5.2*
November 14, 2016	*Password, Authentication and Access Standard*

FAQs

1. **I use my personal computer or mobile phone to access VCU information, does this policy or any other University security policies apply to me?**

   This policy and various other University security policies apply to VCU owned devices and VCU information. While it does not directly apply to how individuals choose to manage their own personal device, it does set expectations for the access of VCU information from those devices. Therefore, if an individual chooses to access VCU information from a personal device, then the access method to the VCU information must be protected in accordance with this policy; where the protection can either be provided from the device and / or from the application designed to deliver VCU information.

2. **My computer or mobile device uses biometrics such as finger print or facial recognition to log me in, is this a viable alternative to having passwords or passcodes?**

   Typically, this is a viable alternative. However, individuals should contact their local IT support personnel, or the VCU Information Security Office, to verify that the method used is appropriate. There are differences in the implementation of biometrics, especially given the changes occurring over time and often, earlier biometrics implementation can now be easily circumvented.

3. **Why must I use a lengthy and complex password? It is impossible to remember all of these passwords we use these days.**

   Generally speaking, the longer the password, the better. For each character added to a password, the password can nearly become exponentially stronger. The VCU Information Security Office recommends the use of a passphrase, where multiple words are chained together to form an easy to remember passphrase. An example of a passphrase would be "Dog8MyDishWash3r", which contains uppercase, lowercase, and numerical characters, and is very lengthy so that it cannot be easily guessed or brute forced. If an individual has trouble remembering multiple passphrases, then a common and effective solution is for the individual to simply insert the service provider name into same passphrase. For example, the VCU passphrase maybe "Dog8MyVCUDishWash3r", and the eBay passphrase can be "Dog8MyeBayDishWash3r".

4. **How can I safely store passwords if I am not supposed to write them down or keep it in a document?**

   While you definitely should not write down your password and leave it unattended, you can store passwords safely with various means. There are digital password vaults and safes that can be used to safely store your passwords; where access to the vault can be protected with a single master password or multi-factor authentication. One such example of an encrypted password database program is keepass. Please inquire with your local IT personnel or contact the Information Security Office within Technology Services.

5. **How can I safely share a password with others?**

   Sharing of your own password for access to VCU Information is not permitted. In some cases, individuals may need to share a temporary password with another individual in the process of granting the other individual access to a system or information. In this case, passwords can be shared with the other individual over the phone, by directly calling the other individual, or via encrypted email (use the word "secure" in email subject line), or via encrypted word document and other encrypted and authenticated file sharing services. Please contact your local IT support personnel or Information Security Office within Technology Services for viable means to accomplish this task if needed.

6. **How can I encrypt my emails?**

   For emails sent using the VCU email systems, simply type the word "secure" in the subject line of your email and your email will be encrypted upon hitting send. Please note this does not work with personal email systems or email systems hosted by other organizations. To learn about the methods used to encrypt emails in other, non-VCU managed email systems, please contact the applicable email service provider.