POLICY TITLE: USER ID AND AUTHENTICATION

(PCI DSS 7.1, 7.2)

Policy Information

Departmental Owner:	Information Technology
Effective Date:	November 8, 2017

Scope

All associates, contractors, consultants, temporary and other workers at Banfield Pet Hospital, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Banfield Pet Hospital, or to devices that connect to a Banfield Pet Hospital network or reside at a Banfield Pet Hospital site.

Definitions

None

Policy Statement

User identification and authentication is vital for the protection of Banfield Pet Hospital's systems, networks, and other resources. Identification and authentication provide accountability and auditability for actions taken by users. The purpose of this policy is to ensure the unique identification of individuals accessing Banfield Pet Hospital information resources and systems.

The following standards were used in development of this policy:

- PCI DSS v3.2
- ISO27002
- NIST

Although Banfield Pet hospital used the foregoing standards in developing this policy, the use of such standards does not mean or imply that Banfield Pet Hospital is subject to such standards.

Policy Requirements

All security policies and procedures must be documented for the restriction of access to cardholder data. See Corresponding Documents for a list of relevant policies. (PCI DSS 7.3)

Banfield standard authentication policies and procedures are to be distributed to all users upon hire. (PCI DSS 8.4.a, 8.4.b) Each new associate at CTS receives an envelope with the 'Welcome to Banfield' instructions for getting started with their computer. The instructions clearly state that installing any software without IT consent is strictly prohibited. The instructions provide the logon name and initial password. The system prompts you to change this initial password at first log on. The requirements for choosing a password are included in the instruction sheet:

- Minimum length: 12 characters
- The password cannot contain the same characters as the username
- Cannot be one of the last 12 passwords used
- Minimum complexity:
  - No dictionary words included
  - You are required to change your password every 90 days
  - Passwords should include at least three out of four of the following types of characters:

- Lowercase letter
- Uppercase letter
- Number
- Special character (i.e. !@#$%^&*(){}[])

The instruction sheet also includes the email address, instructions for changing your password in the future, and the website and phone number for technical assistance.

New hospital associates receive an introductory email. Their hospital leader receives an email with the user name and password format for the new associate. They are given instructions to login for the single sign-on, set their new password, and then they have access to all their learning, FIDO, etc. All associates are presented with this User ID and Authentication Policy during Security Awareness Training, which happens within 90 days of hire and annually. A Learning Management System (LMS) module addresses password security as well.

All systems must have user account management, which involves allocating and administering user accounts. Active Directory is used for network authentication. There are systems that require additional authentication for access.

All user accounts must be based on a unique user identification code (User ID or account). (PCI DSS 8.1, 8.2) Banfield utilizes shared accounts for system and task performance at the hospitals, and some systems require use of the root credentials. Please see the Exception section for more information on the security controls Banfield has put in place.

A unique user identification code (User ID or account) and password is required to access both computers and network resources. (PCI DSS 12.3.2)

All users must authenticate via an automated access control system(s), provided on all system components, when accessing Banfield Pet Hospital IT resources. This access control system shall further invoke a strong encryption method prior to requesting a password. We utilize Active Directory with the standard protections included. (PCI DSS 2.3.a, 7.1, 7.2) User access control is role-based and is restricted to least privilege.

- User passwords shall be changed upon suspicion of compromise, or when a user with privileged access leaves. (PCI DSS 8.4.a, 8.4.b)
- All non-console administrative access must be encrypted using technologies approved by the Information Technology Department such as SSH, VPN, or TLS 1.2. (PCI DSS 2.3)

User ID Naming Convention

(PCI DSS 8.1.a)

Banfield Pet Hospital user IDs shall consist of a unique User ID. All associates hired prior to 2011 have first and last name for their User ID. Associates hired after 2011 are assigned an Oracle ID that follows first initial, last initial, underscore, unique identifier. For temporary associates, the user ID consists of first initial, last initial, underscore, the letter Z, and date of hire (month and day).

ID Uniqueness Conflict

If the above naming convention produces a second non-unique ID, then a letter, in ascending alphabetical order if necessary, will be appended to the end of the duplicate user ID.

Authentication via Password

(PCI DSS 8.2, 8.4.a)

Authentication to access Banfield Pet Hospital IT resources via Active Directory shall be accomplished via the use of user ID and password(s). All such passwords shall be unreadable, during both transmission and storage. Supplementary systems (i.e. Salesforce, Taleo, DayForce, FIDO, etc.) utilize single-sign-on when possible and follow strong password requirements.

User Maintained Passwords

(PCI DSS 8.4.a, 8.4.b)

Users shall ensure the confidentiality of all user IDs and passwords. User IDs and/or passwords shall at no time be disclosed upon request by any individual including Banfield Pet Hospital personnel, IT staff, or management. User IDs and/or passwords shall additionally be prohibited from being recorded in any written form, once the initial user account password has been set. If there is any suspicion that your password has been compromised, please follow the password reset procedures.

Initial Passwords

(PCI DSS 8.2.6)

Initial passwords are to be set to a unique value per user, following the standard set by IT each year (e.g. *a random order of the following: <2-digit month> + <users initials> + <special character> + <unique word theme>)*. The AD checkbox requiring password reset after use is selected. Initial password shall only be valid until the first successful user authentication and must be changed by the user after first use. The user must choose their own passwords based upon the following standards and guidelines.

Password Length

(PCI DSS 8.2.3.a)

All passwords are to be at least 12 characters in length.

Group and Shared IDs/Passwords/Authentication Methods

(PCI DSS 8.5.b, 8.6.a)

Group and/or shared user IDs, passwords, or authentication methods (certificates, tokens, smart cards, etc.) are explicitly prohibited at Banfield Pet Hospital. Any tickets received requesting a Shared ID or access mechanism will be denied. Further, authentication mechanisms are assigned only to an individual account and are not to be shared among multiple accounts. Finally, the authentication mechanisms have physical and/or logical controls defined to ensure only the intended account can use the assigned mechanism to gain access (i.e. RSA tokens with PIN codes). For root credentials and other situations where a shared ID is required and there isn't an alternative, please see the Exceptions section.

Password Expiration

(PCI DSS 8.2.4.a)

Passwords are set to expire every ninety (90) days. Inactive accounts over 90 days old must be removed or disabled.

Password Complexity

(PCI DSS 8.2.3.a)

Password complexity will be set to enforce the use of at least both alphabetic and numeric characters.

- No dictionary words included
- Passwords should include at least three out of four of the following types of characters:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character (i.e. !@#$%^&*(){}[]}

Password History

(PCI DSS 8.2.5.a, 8.4.a, 8.4.b)

Password parameters will be set to require that new passwords cannot be the same as the last twelve (12) previously used passwords.

Multi-Factor Authentication

The use of multi-factor authentication shall be implemented to control access to sensitive information systems or applications both as determined by business or compliance requirements and in accordance with the Banfield Pet Hospital Remote Access Control Policy.

Authentication Lockout

(PCI DSS 8.1.a)

After no more than six failed attempts at authentication for access to an account, the account shall be locked out for a minimum period of 30 minutes or until an administrator resets the account.

Session Timeout

(PCI DSS 8.1.a)

System and session idle timeout feature will be set on all systems to time out after being idle for 15 minutes.

Password Reset

(PCI DSS 8.2.2, 8.2.6)

User identity shall in all cases be verified prior to the completion of any and all requests for password reset. All reset passwords must be set to a unique value and changed by the user after first use.

The following procedures must be followed prior to any non-face-to-face password resets:

1. Verify the users a) Date of Birth and b) last 4 digits of their Social Security Number using FIDO (Oracle ERP tool)

2. Reset the user's password to the temporary password standard for that year *(IT Desktop provides the format each year, a random order of the following: <2-digit month> + <users initials> + <special character> + <unique word theme>)*. The AD checkbox requiring password reset after use is selected automatically.

3. Provide this temporary password to the user over the phone (never via any written source)

4. Verify they can login and change their password successfully

Password Storage and Transmission

(PCI DSS 8.2.1.a)

All passwords must be stored and transmitted with strong encryption. Active Directory uses Kerberos ticketing.

User Access Management

- All additions, deletions, and modifications to user IDs, credentials, and other identifier objects must be controlled. Oracle HRIS creates a report that is passed via batch for all additions and deletions. For modifications to user IDs and credentials, this is a manual notification and process. Desktop requests that a HEAT ticket be filed. (PCI DSS 8.1.a)
- The Information Technology Department will verify that accounts which have been inactive over 90 days have been removed or disabled.
- System privileges related to allowing the modification of production data must be restricted to production applications. Banfield has separate environments for Development, Testing and Production. Access to the environments is based on roles and permissions. Access to production systems for support is requested and approved prior to access, and access is logged.
- All access control systems must have a default "deny-all" setting. (PCI DSS 7.2.3)
- When accessing customer environments for support, different authentication credentials must be used per customer and follow all account and password requirements listed above. (PCI DSS 8.5.1)
- Users are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.

Non-Consumer Customer Passwords:

All non-consumer customer accounts are treated with the Banfield standard Active Directory treatment. In situations where a customer requires a password to access Banfield Pet Hospital systems, the following standards shall be used:

- All non-consumer customer passwords must be changed periodically every 90 days and immediately changed in coordination with Banfield Pet Hospital support notification in the event of suspected compromise. (PCI DSS 8.2.4.b)
  - Guidance must be provided to all customers on when and under what circumstances passwords must be changed.
- All non-consumer customer passwords shall be set to a unique value prior to initial use in alignment with organizational policy.
- All non-consumer customer passwords must be configured to be changed on first use.

- All non-consumer customer passwords must be at least 12 characters long and contain both numeric and alphabetic characters. (PCI DSS 8.2.3.b)
- Non-consumer customer passwords may not be the same as the previous twelve passwords used. (PCI DSS 8.2.5.b)
- Do not communicate the password to the customer in a written or electronic form.
- Non-consumer customer accounts shall be locked out following no more than six invalid login attempts requiring Banfield Pet Hospital support intervention. (PCI DSS 8.1.6.b)
- All passwords must be stored and transmitted with strong encryption. (PCI DSS 8.2.1.d, 8.2.1.e)

Roles and Responsibilities

Roles are assigned to users based on team and title. Responsibilities and access are assigned based on the role of the user. Access is restricted to least privilege: only those functions necessary to fulfill the responsibilities of the job. If the role has a specialty function or need based on a project to which they are assigned, then access can be granted based on that need with written manager approval (through HEAT ticket or email to the system owner). The same process is followed below for Privileged Users. Roles are reviewed at least every 6 months to determine if access need is still required. This review is a function of InfoSec.

Privileged Users

For privileged access to systems, a request is filed via HEAT ticket with business justification and requires manager approval, as well as approval from the system owner or managing team. Privileged users are reviewed periodically per the Auditing and Reporting Policy. Upon separation or termination, privileged user access is disabled with your AD account.

The ability to login as root has been removed from our linux in-scope components. To gain root access, the user must be on the sudoer list and must use sudo to gain access.

For more information on User Roles and Responsibilities, please see the Roles and Responsibilities matrix.

Guidelines

The following guidelines are suggested for the most secure implementation of the User Authentication Policy.

Strong Password Guidance

(PCI DSS 8.4.a, 8.4.b)

Strong passwords have the following characteristics:

Pronounceable Words

Do not use pronounceable words in any language.

Mixture of Characters

Use a mixture of alpha and numeric characters. Consider including special characters and mixing upper and lower case letters.

Passphrases

Consider using a pronounceable word as the base and replace each vowel with a special character or number. For example, base word = stupendous, password = 5tup3nd0u$. You could also consider starting with a phrase you can easily remember (Oh, Say Can You See, By the Dawn's Early Light), and replace each vowel with a special character and mix the case (0sCy$bTd3l).

Protect Your Password

Do not write down your password or share it with anybody.

Do not use the same password for multiple systems.

Do not use information that people would associate with you (such as your name, birthdate, children's names, pet names, etc.).

Reset your password immediately upon notification or suspicion of compromise.

Exceptions

Some internal applications, such as PetWare, have different User ID, authentication and password limitations, as they are not managed by Active Directory, and as such, may not meet the minimum complexity requirements for authentication and passwords, or the password reset requirements. These applications are not accessible via the internet or other public connection and require Banfield network connections.

There are third-party, external applications in use, such as the electronic library available to the hospital doctors, that are not owned or managed by Banfield Pet Hospital. Some of these applications use a group ID for access. In addition, some of these applications do not meet our ID and password requirements, including password resets and strong authentication.

LastPass

Banfield Pet Hospital's User ID and Authentication policy strictly prohibits the use of Shared IDs and Accounts, however there are several systems, machines and network components that have a root login that cannot be changed and must be used, or system and task accounts that run. These instances are not in compliance with PCI DSS v3.2 requirements, and therefore we are implementing a compensating control in the form of a password vault software (LastPass).

This software will provide individual logins to access the root or system account information, which enables audit logging capabilities and a "check out" of the credentials in order to allow Banfield Pet Hospital to determine who was using the credentials in case of an incident. The access will be role-based (only those with a business need for access). The software encrypts the credentials utilizing AES-256 and handles the key management. The software also allows for scanning of passwords to determine if weak passwords are in use, or if passwords need to be changed.

LastPass Enterprise stores access logs for three years and the access logs can be accessed by information security. All shared root credentials are stored in shared folders. Access to the shared folders are using AD groups for access. Information security is the only team that can grant access to the LastPass shared folders. Once a month information security will review the LastPass logs for shared folders. If any unauthorized or unnecessary access to the shared folders are found, the Banfield Pet Hospital security incident process is followed.

Compliance

Violation of this policy may lead to disciplinary action, up to and including separation.

Banfield prohibits taking negative action against any Associate for reporting a possible deviation from this Policy or for cooperating in an investigation. Any Associate who retaliates against another Associate for reporting a possible deviation from this Policy or for cooperating in an investigation will be subject to disciplinary action, up to and including separation.

Corresponding Documents

Privacy Policy

Security Awareness, Training and Education Policy

Remote Access Control Policy

Data Classification and Handling Policy

Encryption Policy

Data Confidentiality Policy

Roles and Responsibilities

Contact

Please reach out to the Information Security Team for questions on this policy. Informationsecurity@banfield.com

Date Last Revised: 3/24/20
Version No.: 1.7