

# How do YOU manage Privileged Accounts?

|                                                    | TechIDManager | DOCUMENTATION<br>MANAGEMENT | PASSWORD<br>VAULTS       | ENTERPRISE<br>SOLUTIONS |
|----------------------------------------------------|---------------|-----------------------------|--------------------------|-------------------------|
| COST                                               | \$            | \$ \$                       | \$ \$ - \$ \$ \$         | \$ \$ \$ \$             |
| PRICE MODEL                                        | # OF AGENTS   | PER USER                    | PER USER                 | PLATFORM<br>ANNUALLY    |
| MARKET                                             | IT PROVIDERS  | INTERNAL &<br>EXTERNAL IT   | CONSUMER -<br>ENTERPRISE | ENTERPRISE              |
| STORES<br>PASSWORDS                                | ✓             | ✓                           | ✓                        | ✓                       |
| CREATION & ROTATION<br>OF PASSWORDS                | ✓             | ✗                           | ✓                        | ✓                       |
| CREATES & DISABLES<br>UNIQUE ACCOUNTS              | ✓             | ✗                           | ✗                        | ✓                       |
| MANAGES ACCOUNT<br>RIGHTS & PRIVILEGES             | ✓             | ✗                           | ✗                        | ✓                       |
| LOCAL ADMINISTRATOR<br>PASSWORD SOLUTION<br>(LAPS) | ✓             | ✗                           | ✗                        | ✓                       |
| OFFLINE CREDENTIAL<br>ACCESS                       | ✓             | ✗                           | ✓                        | ✓                       |
| ZERO-VISIBILITY<br>STORAGE                         | ✓             | ✗                           | ✗                        | ✓                       |
| DOWNTIME<br>TOLLERANT                              | ✓             | ✗                           | ✓                        | ✓                       |
| SELF-HOSTED<br>OPTIONS                             | ✓             | ✓                           | ✓                        | ✓                       |
| DEPLOYS IN:                                        | HOURS         | DAYS - WEEKS                | DAYS - WEEKS             | MONTHS                  |

# Doing the right thing is more than checking a box

**TechIDManager**

HELPS YOU FULFILL THESE SECURITY EXPECTATIONS:

**3.1.1** LIMIT SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, AND DEVICES

**3.1.2** LIMIT INFORMATION SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE.

**3.1.4** SEPARATE THE DUTIES OF INDIVIDUALS TO REDUCE THE RISK OF MALEVOLENT ACTIVITY WITHOUT COLLUSION.

**3.1.5** EMPLOY THE PRINCIPLE OF LEAST PRIVILEGE, INCLUDING FOR SPECIFIC SECURITY FUNCTIONS AND PRIVILEGED ACCOUNTS.

**3.3.2** ENSURE THAT THE ACTIONS OF INDIVIDUAL INFORMATION SYSTEM USERS CAN BE UNIQUELY TRACED TO THOSE USERS SO THEY CAN BE HELD ACCOUNTABLE FOR THEIR ACTIONS.

**3.5.1** IDENTIFY INFORMATION SYSTEM USERS, PROCESSES ACTING ON BEHALF OF USERS, OR DEVICES.

**3.5.7** ENFORCE A MINIMUM PASSWORD COMPLEXITY AND CHANGE OF CHARACTERS WHEN NEW PASSWORDS ARE CREATED.

**3.5.10** STORE AND TRANSMIT ONLY ENCRYPTED REPRESENTATION OF PASSWORDS.

800-171  
800-66

**5.3.13** ENSURE THAT ALL SYSTEM USERS HAVE BEEN ASSIGNED A UNIQUE IDENTIFIER.

**5.2** USE UNIQUE PASSWORDS

**6.2** ESTABLISH AN ACCESS REVOKING PROCESS.

**6.1** ESTABLISH AN ACCESS GRANTING PROCESS.

**6.8** DEFINE AND MAINTAIN ROLE BASED ACCESS CONTROL.

**AC.1.001** AUTHORIZED ACCESS CONTROL; LIMIT INFORMATION SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, OR DEVICES

**AC.1.002** TRANSACTION & FUNCTION CONTROL; LIMIT INFORMATION SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE.

**AC.2.007** LEAST PRIVILEGE; EMPLOY THE PRINCIPLE OF LEAST PRIVILEGE, INCLUDING FOR SPECIFIC SECURITY FUNCTIONS AND PRIVILEGED ACCOUNTS.

**8.1.1** ASSIGN ALL USERS A UNIQUE ID BEFORE ALLOWING THEM TO ACCESS SYSTEM COMPONENTS OR CARDHOLDER DATA

**8.1-1** DEFINE AND IMPLEMENT POLICIES AND PROCEDURES TO PROVIDE ACCURATE USER IDENTITY MANAGEMENT FOR NON-CONSUMER USERS AND ADMINISTRATORS IN ALL SYSTEM COMPONENTS.

**8.1.3** IMMEDIATELY REVOKE ACCESS FOR TERMINATED USERS.

**8.1.5** MANAGE THE IDS USED BY THIRD PARTIES TO ACCESS, SUPPORT, OR PROTECT SYSTEM COMPONENTS REMOTELY.

**8.2.3** PASSWORDS MUST BE AT LEAST 7 CHARACTERS AND CONTAIN NUMERIC AND ALPHABETIC CHARACTERS.

**8.2.4** CHANGE USER PASSWORDS AT LEAST EVERY 90 DAYS.

**8.2.5:** NEW PASSWORDS CAN'T MATCH ANY OF THE LAST FOUR

**8.5** DO NOT USE GROUP, SHARED, OR PUBLIC IDS, PASSWORDS, OR OTHER AUTHENTICATION METHODS.

**8.5.1** ADDITIONAL REQUIREMENT FOR SERVICE PROVIDERS ONLY: SERVICE PROVIDERS WITH REMOTE ACCESS TO CUSTOMER PREMISES SHOULD USE UNIQUE AUTHENTICATION INFORMATION FOR EACH CUSTOMER.

**8.6** AUTHENTICATION MECHANISMS MUST NOT BE SHARED AMONG MULTIPLE ACCOUNTS AND PHYSICAL AND/OR LOGICAL CONTROLS MUST BE IN PLACE TO ENSURE ONLY THE INTENDED ACCOUNT CAN USE THAT MECHANISM TO GAIN ACCESS.

**5.3.13** ENSURE THAT ALL SYSTEM USERS HAVE BEEN ASSIGNED A UNIQUE IDENTIFIER.