DaVinci Academy of Science and The Arts

Policy Number: 702
Policy Section: 700 – Technology

POLICY TITLE: Password Management Policy (Issues and Requirements)

Revision History

Effective Date	Action Date	Revised
8 October 2008	New Policy	New Policy

Password Management Policy (Issues and Requirements)
Effective Date: 17 September 2008
Revision Date:

1. OVERVIEW

This document provides background information, issues, and requirements for designing the DaVinci Academy Identity and Access Management password management solution. The security policy for DaVinci Academy has been updated to implement the following:

- Strong password policy enforcement.
- Intranet password management.
- Extranet password management.

2. ENFORCING PASSWORD POLICY

Requiring users to create strong passwords is a cornerstone of an effective password policy. This requirement must apply to all user accounts at DaVinci Academy.

3. BUSINESS ISSUES

Before DaVinci Academy can expose more of its information infrastructure to partners and other external parties, the school must ensure that its computer systems, network systems and data are well protected. Requiring users to employ strong passwords and change them frequently in Active Directory or in workgroup is a key step to improve the overall security of the network.

4. TECHNICAL ISSUES

The only technical issue for DaVinci Academy is that secure password enforcement should be controlled through the Microsoft Windows desktop and managed centrally through Active Directory Group Policy or via the workgroup scenario.

5. SECURITY ISSUES AND VULNERABILITIES

During the security audit, commonly available tools searched for passwords in Active Directory and work groups that were easy to guess. The results of the audit determined that five percent of all Active Directory user account passwords were blank, and that another 30 percent used very weak passwords such as password, secret, or the user account name. An anonymous user survey found that many users created passwords that an attacker could easily guess because they contained names of family members or pets. Analysis of the password age attribute for the Active Directory and work group accounts also indicated that passwords for many accounts had not changed since the system was deployed 1 year earlier. This means that an attacker carrying out a long-term password guessing or brute force attack, one that is perhaps months or years in length, is more likely to be successful at compromising the account.

6. SOLUTION REQUIREMENTS

6.1 DaVinci Academy translated these issues into the following requirements for the company's password policy:

1. The password policy should enforce regularly-scheduled password changes.
2. Users must create passwords according to the following rules:

    A. Users are not allowed to reuse recent passwords.
    B. Passwords may not contain all or any space-delimited part of the user's account name.
    C. Passwords must be at least eight characters long.
    D. Passwords must contain characters from three of the following four categories:

        English uppercase characters (A through Z)
        English lowercase characters (a through z)
        Base 10 digits (0 through 9)
        Non-alphabetic characters (for example, !, $, #, %)

6.2 Passwords will now move from being "PASSWORDS" to "PASS PHRASES".

An example of a "PASSPHRASE" would be the following:

"Live1ongandProsper!"

This will be a challenge for the Davinci Academy user community; the logistics will be educating the users and working with them to make well remembered "pass phrases".

DaVinci Academy can support these requirements through Active Directory Group Policy or implementation of a strong work group.

7. INTRANET PASSWORD MANAGEMENT

7.1 Business Issues

Many DaVinci Academy users have to use different passwords for the multiple systems that they access daily. Many of these users do not use the same passwords on all systems, so they must keep track of which password to use for which system. DaVinci Academy users have not shown the ability to retain this type of information without writing it down, which means that they often must call the IT Manager to reset their passwords on one or more systems. Synchronizing passwords can address this issue and increase efficiency by reducing the number of passwords that users must remember. In addition, the reduction of password reset requests significantly reduces help desk operating expenses.

7.2 Technical Issues

The solution to the described school and security issues must allow for strong password policy variations for the identity stores that Active Directory and work groups. These variations are often confusing when users try to create new passwords.

7.3 Security Issues and Vulnerabilities

DaVinci Academy is subject to the "sticky note" security vulnerability. Many users post their passwords to different systems in plain view of other employees to remind themselves which password is for which system. Compounding this vulnerability is the fact that users have many passwords for the different systems. Enforcement of a common password policy across multiple systems at DaVinci Academy will reduce the number of passwords that users must remember, which will lessen their need to post sticky notes in the first place.

7.4 Solution Requirements

DaVinci Academy distilled the issues related to password change and synchronization into the following requirements for the company's password policy:

1. Password changes must be synchronized between Active Directory and adjacent systems and service.

2. User-initiated password changes must take place through the Windows Security dialog box, invoked through the CTRL+ALT+DEL key combination. Following this protocol ensures that all users use a single standard password change procedure, because all users run Windows XP, Windows Vista and MAC OS have access to this dialog box.

DaVinci Academy can address these requirements through a combination of Microsoft Identity Integration Server 2003, Server 2008 Enterprise Edition with Service Pack 1 (MIIS 2003 with SP1), using suitable management agents, Active Directory on Microsoft Windows Server™ 2003 and Server 2008 Microsoft Vista and Windows XP clients.

8. EXTRANET PASSWORD MANAGEMENT

Implementing an effective password change strategy for external partners and vendors helps reduce the cost of password management. It also helps increase the security of those passwords by applying the same password policy to all users, not just internal ones. This affects our clients that help with management of of external systems such as our UEN provided hardware and Cisco management consoles.

8.1 Business Issues

DaVinci Academy plans to implement a new password expiration policy for extranet user accounts. This expiration policy requires all users to change their passwords periodically in order to mitigate several types of password attacks.
Currently, the vendors have no way to change their passwords in the extranet domain. DaVinci Academy must provide the tools needed so that extranet users can meet its security requirements as conveniently as possible.

8.2 Technical Issues

DaVinci Academy plan to implement password change management on the intranet does not apply to the extranet. On the intranet, users will use the Windows Security dialog box to change their passwords. This kind of functionality is not available to users who log on to DaVinci's extranet Web applications, so DaVinci must provide a Web-friendly interface through which extranet users can change their passwords.
The password change system must also notify users when their passwords are about to expire so that users can change the passwords before their accounts are disabled. If users do not change their passwords within a certain period after their current ones expire, the old passwords will no longer provide authentication.

8.3 Security Issues and Vulnerabilities

Anytime that passwords are sent across a network, especially a public network like the internet, security is a primary concern. The password change operation must be as secure as possible.

8.4 Solution Requirements

DaVinci Academy translated these password change issues into the following requirements for the company's password policy:

1. Passwords for vendor and partner accounts must follow the School password policy. This applies regardless of whether the partners have access to the intranet.
2. Password changes from the extranet must take place through a secure Web application.
3. Passwords must be transmitted in a secure manner.