Instruction

Administrative Procedure – District #9 Password Procedure

Purpose

Passwords are a critical part of information and network security. Passwords are designed to protect user accounts. A poorly chosen password, if compromised, could place the entire network at risk. As a result, all employees of Granite City School District 9 are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times. The purpose of this procedure is to set a standard for creating, protecting, and changing passwords such that they are (and remain) strong, secure, and protected.

Scope

This procedure applies to all employees of Granite City School District 9 who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any Granite City School District 9 facility, has access to the Granite City School District 9 network, or stores any non-public Granite City School District 9 information. All passwords must conform to the guidelines outlined below.

Password Construction Guidelines

Passwords are used to access any number of district systems, including the network, e-mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Employees should attempt to create a password that is also easy to remember.

1. Passwords should not be based on well-known or easily accessible personal information.

2. Passwords should not be based on a users' personal information or that of his/her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.

3. Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.

4. Passwords should not be based on publicly known fictional characters from books, films, and so on.

5. Passwords should not be based on the company's name or geographic location.

Password Protection Guidelines

1. Passwords shall be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including IT staff, administrators, supervisors, other co-workers, friends, and family members, under any circumstances.

2. If someone demands your password, refer them to this policy or have them contact the IT Department.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's IPsec-secured Virtual Private Network or SSL-protected Web site.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessarily to keep a record of a password, then it must be kept in a secured location if in hardcopy form or in an encrypted file if in electronic form.

5. The "Remember Password" feature of applications should never be used.

6. Passwords used to gain access to district systems should not be used as passwords to access external accounts or information.

7. If possible, do not use the same password to access multiple district systems.

8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately.

9. The IT Department may attempt to "crack" or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Enforcement

An employee who violates this procedure shall be given a reprimand and may be subject to further disciplinary action if the violation(s) are repetitive.

Adopted: 7/25/05