Password policy

1. Overview
Company AS have lately been a victim of criminal activity, and the IT department found it necessary to create a policy that would make Company’s systems more secure.

2. Purpose
The purpose of this policy is to provide a guidance on how to create a secure password, and how Company is supposed to have a secure password at all times. Since we have experienced criminal activities, this is a really important security measure we have to do.

3. Scope
This policy applies to all Company AS employees, partners and other creating a password that is related to Company AS businesses.

4. Policy
4.1 Password protection

- Never write passwords down on notes
- Never send a password through mail, SMS or any other kind of communication
- Never include a password in an unencrypted document
- Never use a password inside the business as a private password
- Don’t use common words in your password
- Don’t use common places or names in your password
- Don’t use a part of your username in your password
- Hide keyboard every time you type the password
- Always check URL at the site where you login to make sure you are at the real site
- If you are suspicious about your password being broken/revealed, please contact IT-department.

4.2 Password Requirements
Setting a strong password is a requirement that is necessary for proper security. This doesn’t make the password impossible to crack, but it does makes it harder. Another thing that is important is that if the password requirements are impossible or too difficult to meet, it would probably decrease security. If they are changed to often, and it has to be complete different every time, most users tend to write them down. This is the password requirements set by the IT-department:

- Minimum-length: 8 characters (This might be changes in the near future because of cracking passwords take a lot less time than before)
- Maximum-length: 14 characters
- Minimum complexity
    - No dictionary words
    - Minimum 1 lowercase
    - Minimum 1 uppercase
    - Minimum 1 number
    - Minimum 1 special character such as !@”#¤%&/()=´}$
- Password is case sensitive, but the username is not
- Password must be changed within 90 days. If it is not changed, the account will be temporary disabled
- Computers should not be unattended with the user logged on and no password protected screen saver active.

4.3 Choosing a password
If you need help creating a password, http://passwordsgenerator.net/ could help you out

4.4 Administration password
The administration passwords should be carefully protected. They shall never be shared and needs to verify login with an email authenticator.

4.5 Protect passwords from attacks

Attackers may capture passwords in several ways, and if someone was to get restricted access to files that contains passwords, these should be stored as one-way cryptographic hashes of passwords instead of the passwords themselves.

5.0 Enforcement

Password security is vital in this company and if an employee doesn’t follow the policies set by Company AS this may be subject to disciplinary action and in the worst case dismissal.