Password Policy

John Hally
John.hally@comcast.net
Why This Policy?

- Very important aspect of security
- Can easily be the ‘weakest link’
- Set standards for:
  - Creation of strong passwords
  - Password protection
  - Frequency of change
Policy Applicability

All:
- Users (local and remote)
- Contractors
- Vendors

Developers
- Their own accounts
- Their applications
  - Support individual user authentication.
  - No clear text password storage
  - Provide role management.
  - Support TACACS+, RADIUS and/or X.509, LDAP security retrieval when possible.
Strong Password Construction

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - “Special” characters (e.g. @#$%^&*()_+|~-==\{}[]:";'<>/? etc)

- Contain at least fifteen alphanumeric characters.

- Are not words in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.
What constitutes a ‘weak’ password?

- Contains less than fifteen characters
- Is a word found in a dictionary (English or foreign)
- Is a common usage word such as:
  - Names of family, pets, friends, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - “<Company Name>“, locations or any derivation.
  - Personal information (birthdays, addresses phone numbers).
  - Word/number patterns - aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
- Above preceded or followed by a digit (e.g., secret1, 1secret)
Password Protection

- Different passwords for non-business accounts - personal ISP, etc.
- Different passwords for various access needs when possible.
- Do not share passwords with ANYONE.
- Should never be written down/stored un-encrypted.
- No passwords in electronic communication (email, chat).
- Do not speak about a password in front of others.
- No hints - "my family name".
- Never on questionnaires or security forms.
- Password demands - refer to this document and/or Information Security Department.
- No ‘Remember Password’ feature of applications.