

# 3M Policies on Computer Usage and Passwords - A Guide for New 3M Employees and 3M Contingent Workers

3M provides computer resources for business use. Any personal use of those resources must be limited within reason, and must not interfere with normal business activities or an employee's ability to meet job expectations.

3M's computer resources must not be used for any purpose which violates the law.

Use of 3M's computer resources must comply with all 3M policies, including those regarding ethical business practices, harassment, use of corporate assets for personal gain, and chain letters.

3M's computer resources must not be used to transmit or store any information which could be considered sexually explicit, profane, threatening, or otherwise offensive.

Only designated spokespersons are authorised to speak publicly on behalf of 3M. Because of this, when posting messages on a public bulletin board users should avoid leaving the impression that they are authorised to represent 3M or that 3M shares their views.

## Users' Responsibility to Maintain Security

Users must control and protect the confidentiality of all passwords, user IDs, and personal identification numbers (PINs) assigned to them or created by them.

Connections to Internet Service Providers (ISPs) must not be installed on a 3M computer for security reasons.

Transmission of 3M Confidential information outside of 3M is forbidden without proper data encryption and non-disclosure agreements.

## The Company's Rights: Monitoring of Usage and Contents

3M reserves the right to access any and all 3M computers, e-mail and Internet usage, by (1) monitoring activity, (2) viewing contents and (3) auditing PC hard-drives.

Computers may be accessed remotely, or physically impounded and audited, at any time and without advance notification. Such audits will be at the discretion of HR and IT Security, and may be random and without any prior suggestion or suspicion of misuse.

## Passwords

Passwords are confidential information and, unless agreed otherwise:

Should be at least 8 keyboard characters long and should not be a dictionary word, not easily identifiable with the user and not easily guessed. This is best ensured by including one or more of the following characters ! \$ & + - \_ ( ) = % ("Special Characters"). In any event the password shall include three of the following categories of characters: Uppercase letters; Lowercase letters, Numerals and Special Characters.

Should not include obvious words such as your name, your employee number, car registration number, or name of spouse / child / dog.

Must not must not be written down, displayed or disclosed.

Must not be stored on the computer, thereby bypassing standard access authorisation; passwords must always be entered manually when accessing any 3M computer system. (i.e. do NOT use any 'Save Password' option).

Must be changed, as a routine at least every 90 days, and immediately if there is any possibility that the password has become known.

Please sign, print your name and date this document below, to confirm your understanding of this document and to acknowledge that whilst at 3M you will always act in compliance with the requirements contained in this document.

.....  
Signed  
.....  
Print name  
.....  
Date