Document Type	Standard
Organization	Business Transformation and Information Technology
Sub Category	IT
Geographic Scope	Global

Title Access Control Standard

Applies To	3M Workers worldwide, workers doing business for or with 3M, and others acting on 3M's behalf. This global standard applies to all locations and situations where 3M business is conducted and to all company sponsored events.
Introduction and Background or Purpose	Access to 3M computing systems is necessary for a wide variety of users to perform their job duties and for the benefit of the corporation. Security and controls must be in place to ensure that such access is granted only to those who need it. Persons with access to 3M systems must ensure that such systems are protected through compliance with all access control standards.
Requirements or Expectations	Access to 3M's network and systems must be, at minimum, controlled with a unique account ID and password combination. 3M workers are held responsible for keeping account and password information secure and confidential. Multi-factor Authentication (MFA) must also be applied in certain situations to ensure that access is granted only to those who are authorized. (See the Multi- Factor Authentication Standard). Access to 3M systems or information must be authorized, at a minimum, by the user's management and by the owner/custodian of the system, application or data. There are only three situations where an approved proxy for these authorizers may be used. 1) for company executives, 2) for bulk loading of users during acquisition cutovers, 3) for access deemed a birth right for workers. Access rights must be limited to the lowest level needed to perform assigned tasks. Access must be documented, including listing of specific privileges approved, and treated as need to know information. Access to host operating systems must be controlled. Logging and/or monitoring must be used to ensure that only authorized personnel are accessing 3M information. Access to 3M computing systems must include a method to identify and validate users of those systems. Access to administrative system commands must be restricted to specific qualified persons who have been authorized by 3M management to perform

	duties requiring elevated permissions. Separate accounts must be used distinct from the person's general user account to facilitate clear separation of roles/responsibilities. Accounts that have elevated privileges must follow the Password Vault Standard. Access must be reviewed periodically to ensure such access is still required. Access to another individual's electronic data on 3M systems may be made available only to persons who have been authorized to receive such data. Access through any mobile devices, including laptop computers, smart-phones, tablets and similar devices requires that the devices be configured with approved security measures to protect 3M intellectual property, systems, networks and applications. Approved security protective measures must be defined and implemented in remote access systems and services such as VPN. Assignment of access should be based on individual personnel's job classification and function. Access must be authenticated, at minimum, through a combination of an account and password. Managers / Supervisors are accountable for ensuring access is revoked when such access is no longer required, such as changes in responsibility or terminations. Managers / Supervisors are accountable for ensuring access is revoked and/or removed and reported if inappropriate usage is detected. Overall responsibility for compliance with this document is assigned to the 3M Chief Information Security Officer. Failure to comply with these requirements may result in discipline up to and including termination of employment.
Additional Elements	Local workstation and/or server administrator accounts must be controlled and blocked from using Remote Desktop Protocol (RDP), unless the account is managed in the corporate password vault. Birth right access is access that is automatically granted when a 3M worker is on-boarded (based on Human Resource records), or otherwise deemed necessary for all workers. All capable systems and devices must be configured to revert to screensaver

and/or shut down during idle time or inactive sessions after a defined period of inactivity.

For high-risk applications, all capable systems must be configured with restrictions on connection time(s) to provide additional security.

Access to 3M Systems may be controlled/managed by the use of roles or groups. The following principles apply to roles/groups, their owners, and custodians:

- Role/groups must have at least one custodian that is a 3M Employee. That custodian will be considered the Role/group owner.
- The role/group owner is accountable for actions associated with that role/group.
- The role/group owner may delegate day-to-day management responsibility of the role/group to a non-3M worker custodian.
- Some role/Groups (such as those designated for Export Controlled systems) have special requirements governed by regulations that must be met. Role/Group owners and custodians for those groups must meet all applicable personal eligibility requirements.
- Role or Group membership requests must be approved by either Owners or a Custodian.
- Persons designated as Group Owners and Custodians must be reviewed periodically. An owner or a custodian may not approve themselves for that role.

Code of Conduct	BE LOYAL: Electronic Resources
Linked Documents	Information Security PolicyMulti-Factor Authentication (MFA) StandardNetwork Access Control StandardPassword Vault Standard
Other Reference	
Further Information	Scott Sitowski; IT Manager; Information Security, Risk & Compliance John Noll; IT Manager; Information Security, Risk & Compliance Carl Fassbender; IT Manager; Information Security, Risk & Compliance
Original Issue Date	11/1/2013
Last Reviewed Date	3/8/2018