

Information Security and Confidentiality

Policy statement

Employees and others acting on 3M's behalf are responsible for protecting 3M's confidential information from unauthorized disclosure whether internal or external, deliberate or accidental. Employees and others acting on 3M's behalf must know:

- The information classification of the 3M information they create or have access to (3M Confidential Information, Internal Use Only, or External Release)
- The security precautions that apply to 3M information, and
- How long to retain 3M information, and how to properly dispose of it.

Just as we expect others to respect our company's confidential information, 3M respects the confidential information of other parties. It is 3M policy to use only legal and ethical means to collect and use business and market information in order to better understand our markets, customers and competitors. 3M will not collect or use another party's confidential information without that party's permission.

What it means for 3M confidential information

- Protect 3M confidential information regardless of the media in which the information is conveyed (e.g., printed, electronic files, e-mail, verbal conversation).
- Protect 3M confidential information for the entire life cycle of the information--from creation, storage, use, transmittal, retention through disposal.
- Contact your assigned 3M legal counsel if you need help determining whether certain information is confidential.
- Share confidential information inside 3M only with those who have a business need to know the information.
- Have a written, signed confidential disclosure agreement before disclosing confidential information to a party outside 3M. Confidential disclosure agreements must be signed by a general manager or technical director, or higher level.
- Wear your 3M identification badge while at 3M facilities and ensure that others are authorized to be in your area and are authorized to have access to 3M business information.
- Retain all 3M information in accordance with 3M's Records Retention Schedule. If you have received a Preservation Notice, immediately take steps to preserve all potentially pertinent records and files.
- Promptly report any actual or suspected unauthorized access to 3M systems or 3M information to:
 - Your manager,
 - Corporate Security at 651-733-6100 (available 24 hours)
 - IT Security and Integrity. List of local Information Security Contacts

- 3M Business Conduct Compliance at 1-877-3M-ETHICS in the U.S. or 3M-Ethics.com (for web reporting or worldwide telephone reporting)
- The 3M Director, Business Conduct and Compliance
- The assigned 3M legal counsel for Information Technology

What it means for confidential information of others

- As we do not disclose 3M confidential information without a proper confidential disclosure agreement, do not accept another party's confidential information without a written, signed confidential disclosure agreement. These confidential disclosure agreements must be signed by a technical director or higher level executive.
- Unless you have another party's permission to use the party's information, make sure you can answer "no" to each of these questions before using the information:
 - Is the information actually confidential information?
 - Was the information obtained illegally or unethically?
 - Would using the information violate any other business conduct policy?
- Contact your assigned 3M legal counsel before hiring or using a consultant or agent to obtain information for 3M or if you learn that an improper disclosure or improper use of another party's confidential information may have occurred.
- Do not interview or hire employees or consultants of competitors without first contacting your assigned legal counsel.