SECURITY POLICY
For: Morreale Companies

Effective March 2015

STATEMENT

The Morreale Companies possess information that is sensitive and valuable such as personally identifiable information, financial data, and other information considered sensitive. Some information is protected by international, federal, and state laws or contractual obligations that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the Morreale Companies, and could also subject the Morreale Companies to fines or other government sanctions. Additionally, if Morreale Companies' information were tampered with or made unavailable, it could impair the Morreale Companies' ability to do business. The Morreale Companies therefore require all employees to diligently protect information as appropriate for its sensitivity level.

Failure to comply with this policy may be subject to disciplinary measures.

MORREALE COMPANIES' SUMMARY OF RESPONSIBILITIES

Employees and/or Contractors:

1. Employees and/or Contractors may only access information needed to perform their legitimate duties in their capacity and only when authorized.
2. Employees and/or Contractors are expected to ascertain and understand the sensitivity level of information to which they have access.
3. Employees and/or Contractors may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized within the scope of their professional activities.
4. Employees and/or Contractors must understand and comply with requirements related to personally identifiable information (PII).
5. Employees and/or Contractors must adhere to requirements for protecting any computer used to conduct company business regardless of the sensitivity level of the information held on that system.
6. Employees and/or Contractors must protect the confidentiality, integrity and availability of the company's information as appropriate for the information's sensitivity

level wherever the information is located. (held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.)

7. Information deemed Confidential under this policy must be handled in accordance with the requirements for protecting Confidential Information.
8. Employees and/or Contractors must safeguard any physical key, ID card or computer/network account that allows them to access company information. This includes creating difficult-to-guess computer passwords.
9. Employees and/or Contractors must destroy or render unusable any confidential information contained in any physical document (e.g. memos, reports, printed digital document) or any electronic, magnetic or optical storage medium (USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.
10. Employees and/or Contractors must report any activities that they suspect may compromise sensitive information to their supervisor or to the IT Manager.
11. While many international, federal, and state laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, any Employee and/or Contractor who receives such compulsory requests should contact their manager before taking any action.
12. If Employees and/or Contractors are performing work in an office that handles information subject to specific security regulations, they are required to acknowledge that they have read, understand and agree to comply with the terms of this policy annually.

Managers and/or Supervisors: In addition to complying with the requirements listed above for all employees and/or contractors, managers and/or supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity, and availability defined by the Information Guardian and designees, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each employee and/or contractor understands his or her information security-related responsibilities.

IT Managers: In addition to complying with the policy requirements defined for all employees and/or contractors, and managers and/or supervisors, those individuals that are assigned to manage computing and network environments that capture, store, process and/or transmit information, are considered IT Managers and are responsible for ensuring that the requirements for confidentiality, integrity and availability, as defined by the appropriate Information Guardian, are being satisfied within their environment. IT Manager responsibilities include but are not limited to:

1. Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
2. Developing, implementing, operating, and maintaining a secure technology environment that includes:

    a. A cohesive architectural policy.

    b. Product implementation and configuration standards.

    c. Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Guardians.

    d. Developing an effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.

3. Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

Information Guardians: In addition to complying with the requirements defined for all employees and/or contractors, managers and/or supervisors, and IT Managers, those individuals assigned to guard Companies' held information are considered Information Guardians. Information Guardian responsibilities include but are not limited to:

1. Working with the IT manager to understand the restrictions on the access and use of information as defined by federal and state laws and contractual obligations.
2. Defining the confidentiality, integrity, and availability requirements (sensitivity level) for each piece of information.
3. Conveying in writing the sensitivity level of each piece of information for which he or she is responsible for to the managers of departments that will have access to the information.
4. Working with department managers and/or supervisors to determine what users, groups, roles, or job functions will be authorized to access the information and in what manner (e.g. who can view the information, who can update the information).

MORREALE COMPANIES' REQUIREMENTS AND DEFINITIONS

Information Collections and Guardians: Companies' held information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable international, federal, and state laws, the Companies' contractual obligations, and with the information's significance to the company as well as any individual whose information is collected. Achieving this objective requires that:

1. The information's sensitivity level must be defined to convey what level of protection is expected to all employees/agents who are authorized to access the information.
2. The individuals who should have access to sensitive information must be identified, either by role or by name.

For purposes of managing information, the various types of information must be segregated into logical collections (e.g. power of attorney, employee benefit data, payroll data, or financial records). Each collection must be "managed" by an individual known as an "Information Guardian," who must:

1. Define the collection's sensitivity level consistent with this policy.
2. Convey the collection's requirements to the managers of departments that will have access to the collection.
3. Work with office heads and chairs to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g. who can view the information, who can update the information).

Information Sensitivity Levels: Information Guardians are responsible for assessing the security requirements for each of their assigned information collections across three areas of concern: confidentiality, integrity and availability.

To facilitate the assessment process and ensure that these requirements are expressed in a consistent manner across the company, Information Guardians should categorize their information collections using the levels described in this section.

The **confidentiality** requirement for an information collection will be expressed in the following terms:

1. "**Public**" information can be freely shared with individuals without any further authorization by the appropriate Information Guardian/designee.
2. "**Internal**" information can be freely shared with members of the company. Sharing such information with individuals outside of the company requires authorization by the appropriate Information Guardian/designee.
3. "**Confidential**" information can only be shared on a "need to know" basis with individuals who have been authorized by the appropriate Information Guardian/designee, either by job function or by name.

The **integrity/availability** requirement for an information collection will be expressed as follows:

1. Information is "**Non-critical**" if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support

staff, and incur limited recovery costs. Reasonable measures to protect information deemed "non-critical" include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.

2. Information is "**Critical**" if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the company to:

    a) Suffer significant financial loss or damage to its reputation,
    b) Be out of compliance with legal/regulatory or contractual requirements,
    c) Adversely impact its clients.

3. Additional safeguards for "**Critical**" information:

    a) **"Critical"** information must be verified either visually or against other sources on a regular basis, and
    b) A business continuity plan to recover **"critical"** information that has been lost or damaged must be developed, documented, deployed and tested annually.

Personally Identifiable Information (PII): Personally Identifiable Information (or "PII," as used in this Policy) is information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc. All Personally Identifiable Information in the possession of the company is considered Confidential unless:

1. The information is designated as "Directory Information" by the appropriate Information Guardian; or
2. The Information Guardian has otherwise authorized its disclosure.

Managers and/or Supervisors must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals and on a need to know basis.

Requirements for Any Computer Used to Conduct Company Business: In order to adequately protect company information systems from compromises, all computers used to conduct company business must be configured using security industry-sanctioned best practices that include but are not limited to the following:

1. Configuring and using computers in a manner that is compliant with the company's core technology policy
2. Requiring all computer accounts to have strong passwords as defined by the company's password policy
3. Define accounts intended for day-to-day computer use as "general user accounts". Accounts that have administrative privileges must only be used for system setup and maintenance.
4. Computers should be configured to "time out" after no more than 20 minutes of inactivity.
5. Users should lock or log off their computers before leaving them unattended.
6. Ensuring that system and application security updates are applied as soon after being released by the vendor as possible.
7. Ensuring that anti-virus software is installed and is actively protecting the system.
8. Ensuring that any system is configured to keep a record of:
    a) Who attempted to log into the system (successfully and unsuccessfully) and when,
    b) When they logged out,
    c) Administrative activity performed,
    d) Unsuccessful attempts to access confidential files.

Managing Confidential Information: No one may access information that has been classified as Confidential without authorization by the appropriate Information Guardian. For information classified as Confidential, such authorization may be granted to individuals by name or to all individuals serving in a specific job function. For information classified as Highly Confidential, access must be authorized for each individual by name.
For information classified as Confidential, the following procedural and system-level controls must be in place:

1. Access to a confidential information collection may only be granted after receiving permission by the appropriate Information Guardian/designee authorizing such access.
2. Departmental procedures must be in place to ensure that all individuals who have access to Confidential information are aware of the sensitivity of the information to which they have access, understand their responsibilities to protect that information appropriately, and acknowledge their understanding and intent to comply with this policy.
3. Tangible records (paper documents, microfilm, etc.) containing Confidential or Highly Confidential information must be stored in a locked cabinet or drawer when not in use with access limited to authorized individuals, and physically shredded/destroyed when no longer needed. In addition to the requirements for all computers used to conduct company business, computers that accept, capture, store, transmit or process information classified as Confidential. Any piece of Confidential or Highly confidential

information that is transmitted across the internet must be encrypted using an encryption product and methodology approved by the company IT manager.

4. Computer servers must be secured by a hardware firewall, approved by the IT manager, which only permits connections with authorized systems using approved protocols.

Agreements protecting Company information: When negotiating contracts with external entities, company employees will consider whether there are any alternatives to giving members of the other organization access to company databases or to other filing systems containing sensitive information.

If such access is necessary, agreements that provide the outside entity with access must ensure that the employees/agents of the entity are required to maintain confidentiality consistent with the company's obligations and interests. In addition, outside employees/agents should be contractually obligated to implement data protection and security measures that are commensurate with the company's practices.

Security Policy Revision Log

Version	Date Issued	Reason for Update
Original	10/22/2014	
Update	11/11/2014	Removed redundant wording
Update	12/01/2014	Formatting
Update	5/1/2017	Reapproved