Information Security Policy

Number	IT101
Policy Owner	Information Security
Approved By	Chief Information Officer

Effective Date	12.31.2011
Last Revision Date	04.19.2023
Page	1 of 7

PURPOSE

. Information is a critical Company asset and as such must be protected from misuse, improper access, and delays in processing. It is imperative that the following policy be implemented and enforced to ensure the confidentiality, integrity, and availability of Company Information.

Company Information must be protected in a manner commensurate with its sensitivity, value and critical nature. Security measures must be employed regardless of the medium on which Information is stored (i.e., paper, PCs, Workstations, Mobile Devices, Removable Media, etc.), the systems which process it (i.e., PCs, networks, voice mail systems, etc.), or the methods by which it is moved (i.e., email, paper, face-to-face conversation, etc.). Such protection includes restricting access to Information based on the need-to-know.

SCOPE

This document applies to Select Medical, its subsidiaries and affiliated companies and all personnel accessing Company Property.

RESPONSIBILITY

Supervisors and managers are responsible for keeping all Workforce members informed of this policy. All Workforce members will be informed of this policy through new-hire orientation and annual compliance training thereafter and will be required to acknowledge and abide by the policy.

DEFINITIONS

Company: Select Medical and its subsidiaries, affiliates, and joint venture entities managed by Select Medical Corporation.

Company Property: All right, title and interest in or to the Hardware, Software, Information, or Data owned, leased, or licensed by the Company.

Corporate Confidentiality Statement (must be used verbatim)**:** Note: The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to the message and deleting it from your computer. Thank you.

Data: Raw, unorganized facts that may be captured, stored, processed, and/or transmitted.

Encryption: Encryption is the conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties.

Hardware: All tangible equipment and media used in the capture, storage, processing, transmission, and presentation of Information and Data, including, but not limited to workstations, endpoints, mobile devices, information storage media of any kind, information presentation products, medical devices, and network equipment.

I.S. Help Desk: A team of dedicated resources who provide end users with information and support related to the Company's IT systems. Also known as the IS Solution Center.

Information: All processed, organized, structured, and/or contextualized Data that may be captured, stored, processed, or transmitted.

Information Security: The internal Information Services department responsible for architecting, implementing and managing all aspects of the Company information security program including, but not limited to Security Technology, Operations and Incident Response, Governance, Risk and Compliance, and Identity and Access Management .

Information Services (I.S.): The internal department responsible for delivering exceptional services; creating change with innovation through process and technology; and building trust with the business to drive strategic and operational goals.

Mobile Device: Any electronic computing and communications device which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information.

Non-sensitive Data: Data or Information that can be shared with all audiences without restriction or concern for disclosure.

Owner of Information: The individual or entity who has a vested interest in, who has been given the authority to allow access to, and who has the responsibility of maintaining the integrity of the Information.

Password: A secret phrase or combination of alphanumeric characters that must be used to gain access to a computer, application or electronic device. A password can also be referred to as a “passphrase.”

Personal Computer (PC): Any laptop, notebook, desktop, thin-client, smartphone or any other personal computing apparatus or device which is used to access, process or display

information. This definition does not include computing devices operating as servers in a hardened, controlled access, secured data center.

Personally Identifiable Information (PII): Any personally identifiable information in any media or form about or relating to any identified or identifiable individual, including, but not limited to, personal health information or medical records, personal financial information, social security numbers, driver's license numbers or state ID card numbers, financial account numbers, security codes, access codes, passwords, personal identification numbers, credit card or bank account numbers, credit card verification codes, credit card expiration dates, and any credit card magnetic stripe data, home address and home telephone number; device IDs; e-mail addresses; billing information; and individual usage history. PII includes directory information (such as work addresses, telephone numbers, and e-mail addresses) and other types of personal information. PII includes data classified as HIPAA PHI.

Proprietary Data: Data that is owned by Company that allows it to control and safeguard its competitiveness over other companies.

Protected Health Information (PHI): Data that generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Removable Media: Any portable storage device including, but not limited to, backup tapes, CDs, DVDs, USB/flash drives, memory cards, hard drives, portable media players, smart phones, and cameras.

Sensitive Data: All PII, PHI, and Proprietary Data.

Shadow IT: The use of IT-related Hardware, Software and or cloud services by a department or individual without first obtaining the appropriate approval(s) from Shared Services.

Shared Services: The main operational groups for the Company's executive, managerial, Human Resources, Communications, Operations, Procurement, Finance, Legal and Accounting, Information Services, Central Business Office and other relevant departments that provide enterprise-wide support.

Software: All computer programs, applications, operating systems, languages, commands, or utilities used in the storage, processing, retrieval, or transmission of Information and Data.

System Fault: An abnormal condition or defect at the component, equipment or sub-system level which may lead to a failure.

UserID: The unique identifier, protected by a changeable Password, which identifies each computer, application, and/or system user.

Workforce: Employees of Select Medical and its subsidiaries, affiliates or entities it manages or controls, volunteers, students and trainees, agency staff, vendors, consultants, contract staff and others whose work performance is under the direct control of Select Medical or its subsidiaries, affiliates or entities it manages or controls.

Workstation: A desktop, laptop, tablet computer, thin client and/or server.

POLICY

It is Company policy that:

A. All Information and Software that processes Data (which include programs making up operating systems) are Company Property. Company forbids either the Information or the Software to be given to or viewed by anyone not authorized by Company.
B. Unless for an approved business process, no Information, Data, or Software shall be downloaded, transferred or otherwise made available to non-Company Hardware or any non-Workforce member without prior permission from Information Security through the Workforce member's immediate supervisor and senior leadership.
C. At minimum, the following steps shall be taken to protect Company Information:
    1. Control and limit physical access to areas containing Information and/or Data processing resources, to essential personnel.
    2. Provide only the level of access necessary (READ, MODIFY and or DELETE) to those Workforce members with the need to use the Information.
    3. Provide necessary procedures to ensure that the transferal or termination of a Workforce member's access is in accordance with their roles and responsibilities within the Company.
    4. Provide necessary tools to monitor and enforce security policies.
    5. Implement and maintain documented procedures to impede or prevent Workforce members or third parties from tampering with or misusing Information.
D. All Company Property shall remain the property of Company, regardless of its origin, including, but not limited to, any Software or Data developed by Workforce members for Company or using Company Property. The Workforce member hereby assigns to Company the entire right, title, and interest in and to any Software or Data developed by the Workforce member for Company, and shall execute any assignments or other documents necessary to effect such assignments. The Workforce member agrees that any Software or Data developed by the Workforce member for Company or using Company Property shall be deemed a "work made for hire".
E. No electronic devices connected to Company Property, including but not limited to broadband, dial-up, VPN, or SSL connections from remote locations, shall be left unattended while signed on unless Password protected.
F. Each Workforce member must ensure that remote connections to Company assets are logged off when not in use and not left unattended unless Password protected.
G. All remote connections should require the user to enter a UserID, Password and where feasible, two-factor authentication to gain access, and should not make use of any type of

feature that would bypass this requirement unless a feature is specifically approved by the Chief Information Officer or Chief Information Security Officer.

H. Remote and/or local area network layer connections to Company's internal network resources are only permitted from Hardware owned by Company, unless authorized by Information Security.
I. Connecting any device or cloud service not issued, or previously approved, by the Information Services department to any Company equipment (workstations, servers, tablets, etc.), even for the purposes of providing power, is prohibited, unless authorized by the Information Security department. If these or any other Shadow IT activities are identified, Company has the right to block such activities and enforce disciplinary action, as deemed appropriate by Company.
J. While using Company Property, connections to the internet must not be left unattended, and internet browsers should be closed when not in use.
K. When on Company premises the Workforce member shall not use or install any personal locks on any Hardware, safes, or storage cabinets, or on any adjacent office equipment. Company reserves the right to inspect the Workforce member's work area and remove, by any means, any personal locks found to be installed in violation of this policy.
L. When working remotely, personal locks may be used in order to lock and store Company Information away from unauthorized individuals. This can be via room, closet, drawers or cabinet.
M. The Workforce member shall be solely responsible for any computer activity conducted under the Workforce member's UserID, and shall not disclose such UserID and associated Password to anyone, unless authorized beforehand by a member of Information Security. The Workforce member shall not in any way attempt to discover the Password of any other Workforce member.
N. The Workforce member shall not use any Company Property, in whole or in part, for personal reasons, unless authorized by the Workforce member's immediate supervisor.
O. Testing of security systems is prohibited without approval of the Chief Information Officer or Chief Information Security Officer. Disclosing, capturing, altering, or destroying Information that relates to or creates security exposures is prohibited. All security exposures must be disclosed to the Chief Information Officer or Chief Information Security Officer as soon as possible. Additionally, Workforce members are prohibited from disclosing, changing, or disabling any audit features without the approval of Information Services.
P. Workforce members must report all system errors/issues with Company owned assets or systems to the I.S. Help Desk.
Q. The Workforce member shall not use any Company Property to gain unauthorized access to any Software or Data, whether the property of Company or a third party.
R. The Workforce member shall not unduly influence or attempt to influence Company to purchase, lease, or license any Hardware, Software, or Data from a third party vendor with which the Workforce member has had prior dealings.
S. Workforce members should not expect privacy with respect to any use of or access to Company Property. Company reserves the right and has the legal authority to review any Data files, web or application activity, messages, or communications sent, received, or

stored on Company Property. Workforce members will adhere to applicable laws and industry standards while utilizing Company equipment wherever they are physically located, including when they are on Company Property or working remotely.

T. The environments containing Company Information and Data processing resources shall be adequately protected by using appropriate procedures and technology. Some examples of these would be locked doors or cabinets, fire alarms, suppression devices, and emergency power supplies.
U. All departments that process and maintain Company Information shall ensure that a documented contingency plan is developed to enable the continued availability of important or critical Information in the event of an extended emergency.
V. Unless it has specifically been designated as Non-sensitive Data, all Company Sensitive Data must be protected from disclosure to third parties. Third parties may be given access to Company Sensitive Data only when demonstrable need-to-know exists, when a Company contractual agreement has been signed, and when such a disclosure has been expressly authorized by the relevant Company Owner of such Data. If Sensitive Data is lost, or disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, Information Security and Compliance must be notified immediately.
W. All Workforce members who secure Company Property with Passwords or Encryption shall turn over the Passwords or decryption keys to Information Security upon separation from Company.
X. If remote access to Company's internal network resources is granted, the Workforce member must maintain a work environment that meets security and confidentiality requirements for interacting with Sensitive Data as defined by Company's policies and procedures as well as established law. Workforce members must not compromise the confidentiality or security of Information due to remote computer access. Workforce members must ensure that Sensitive Data in any form cannot be accessed, viewed and/or heard by any unauthorized person. It is the Workforce member's responsibility to be aware of their surroundings when viewing Sensitive Data regardless of location.
Y. Any paper and or notes generated for work need to be properly shredded. If working remotely it is preferable that the paper or notes generated for work be taken to a Company location and placed in a shred bin.
Z. Breaches in the use and handling of Sensitive Data or technology, whether intended or unintended, will be subject to disciplinary action up to and including termination, in accordance with Company's Human Resources policies, procedures and Code of Conduct.
AA. The Workforce member shall use any Software purchased, leased, or licensed from third party vendors strictly in accordance with the license agreement and copyright statements for such Software. The Workforce member shall not copy, download or upload any such Software without the prior approval of Information Security, and shall not under any circumstances modify any such Software.
BB. The Workforce member acknowledges that any action taken by the Workforce member in violation of this policy may subject both the Workforce member and Company to criminal and civil liability. In the event that any suit, claim, or demand is asserted against Company which arises out of the Workforce member's actions in violation of this policy, the Workforce member shall indemnify, defend, and hold harmless Company from and

against all liability, cost, or expense, including attorney's fees. The indemnity contained herein shall survive the expiration or termination of the Workforce member's employment with Company.

The Workforce member acknowledges that any violation of the above rules and procedures may subject the Workforce member to disciplinary action, including, but not limited to, termination of the Workforce member's employment and civil and criminal proceedings. In the event that the Workforce member's employment is terminated, the Company shall retain all legal or equitable remedies against the Workforce member, and such remedies shall be cumulative and not exclusive.

No set of policies and procedures can be crafted to cover every potential situation that employees might face in the day-to-day conduct of Select Medical's operations. The policies and procedures set forth in the Information Security Policy documents are written in broad terms and are intended to serve as guidelines for situations that employees may encounter. Nonetheless, situations may arise which are not addressed by the Information Security Policy documents or which raise questions as to the appropriate application of legal or regulatory requirements. When in doubt, you should consult with Legal, Compliance or your supervisor before taking any action.