INFORMATION ACCESS POLICY

1. OVERVIEW

An Information Access Policy sets company policy on controls required to ensure security of information residing in its possession.

2. PURPOSE

The purpose of this policy is to maintain an adequate level of security to protect Perimatics data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of Perimatics information systems.

3. SCOPE

This policy applies to all Perimatics employees and affiliates.

4. POLICY

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

4.1 Who is Affected:

This policy affects all employees of this Perimatics and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

4.2 Affected Systems:

This policy applies to all computer and communication systems owned or operated by Perimatics and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

4.3 Entity Authentication:

Any User (remote or internal), accessing Perimatics networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff
- Unique user identifier
- At least one of the following:
  - Biometric identification
  - Password
  - Personal identification number
  - A telephone callback procedure
  - Token

4.4 Workstation Access Control System:

All workstations used for this Perimatics business activity, no matter where they are located, must use an access control system approved by Perimatics. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOs. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 30 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

4.5 Disclosure Notice:

A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.

4.6 System Access Controls:

Access controls will be applied to all computer-resident information based on its' Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

4.7 Access Approval:

System access will not be granted to any user without appropriate approval. Management is to immediately notify the Security Administrator and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.

4.8 Limiting User Access:

Perimatics approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.

4.9 Need-to-Know:

Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.

4.10 Compliance Statements:

Users with access to the Perimatics' information systems must sign a compliance statement prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by these Perimatics policies and procedures related to computers and information systems. Annual confirmations will be required of all system users.

4.11 Audit Trails and Logging:

Logging and auditing trails are based on the Data Classification of the systems.

4.12 Confidential Systems:

Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access

- All privileged commands must be traceable to specific user accounts

In addition, logs of all inbound access into Perimatics 's internal network by systems outside of its defined network perimeter must be maintained. Audit trails for confidential systems should be backed up and stored in accordance with Perimatics back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.

4.13 Access for Non-Employees:

Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the Perimatics computers or information systems unless the written approval of the CIO has first been obtained.

4.14 Unauthorized Access:

Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of 'production data' must be restricted to 'production' applications.

4.15 Remote Access:

Remote access must conform at least minimally to all statutory requirements including but not limited to HIPAA.

5. POLICY COMPLIANCE

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Revision History

Date of Change	Responsible	Summary of Change
Dec 2018	COO	Updated and converted to new format.