Dominion Dental USA, Inc. and Subsidiaries

POLICY TITLE	**COMPUTER USE AND INFORMATION SECURITY**
POLICY NUMBER	**IT-110-D**

Original Issue Date:	March 2014
Effective Date of Prior Version:	March 2017
Last Review Date:	November 20, 2018 ☒ Updated □ No Update
Next Scheduled Review Date:	November 20, 2019
Owner:	Information Technology ("IT")

I. DESCRIPTION/BACKGROUND

This policy applies to Dominion Dental USA, Inc. and its directly and indirectly owned subsidiaries d/b/a Dominion National (hereinafter referred to as "Dominion").

This policy assists Dominion in providing a business aligned security program that meets its operational, compliance, and information security needs to protect the confidentiality, integrity, and availability of information, data, and the supporting systems.

Employees and contractors must follow this policy. Any exceptions to this policy must be documented as an exception request. Please see the Exceptions section of this policy for additional guidance related to policy exception requests.

II. DEFINITIONS

Access
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative/Operational
Administrative or Operational accounts are typically used to administer or configure the system. Further, the person (or program) must go through an authentication process (such as supplying a password) in order to utilize this account. For such accounts, the password is often shared among a group of administrators. Once approvals have been granted to create this account, the responsible department must ensure that an individual is assigned ownership for the Operator ID from each work shift throughout the day.

Authentication
The corroboration that a person is the one claimed.

Confidential Information
Information prepared, generated, received, and/or maintained in written or electronic form by Dominion with the expectation of Dominion and/or another party (e.g., member, provider, or employee) that the information will be kept private and will not be disclosed to unauthorized parties. Please see the Code of Conduct for additional guidance related to confidential information.

Corporate Computing Environment
Various methods of electronic data storage, data processing, and data communications used for business operations.

Electronic Protected Health Information
This is patient identifiable health information that is transmitted by electronic media or maintained in electronic media.

Electronic Media
Electronic storage media including memory devices in computers (hard drives) and any removable transportable memory medium, including, but not limited to, magnetic tape, disk, optical disk, digital memory card, etc. It also includes transmission media used to exchange information already in electronic storage media, such as the Internet, leased lines, dial up lines, private networks, etc.

Encryption
A process that transforms data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Incident
An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the corporate computing environment.

Individual User Account
A unique user identifier (user ID) that is associated with an individual or an information system.

Protected Health Information ("PHI")
Individually identifiable health information which is transmitted or maintained in any form (verbal, paper, electronic) which can be used to identify an individual who has Dominion's coverage. Please see HR-0735, Privacy of Member Information for additional guidance related to protected health information.

Proprietary Information
Information that is the property of Dominion and is to be used for business purposes only as deemed appropriate by Dominion. Please see the Code of Conduct for additional guidance related to proprietary information.

PST Data File
A file format used by Microsoft Outlook to store local copies of messages, calendar events, and other items.

Segregation of Duties
A process to divide sensitive actions or transactions among multiple individuals to prevent unauthorized or inadvertent errors or changes.

System Account
A System Account is used to run a service/daemon/started task/etc. The system/application executes with the privileges of this account in order to accomplish its task. Such accounts are not typically used by administrators for administrative tasks on a regular basis although the account may be needed for some very privileged tasks in the system/application. The supervisor of the unit that is responsible for administering the system typically assigns ownership for this type of account.

Virus and Malicious Software
Software that is designed to damage or disrupt an information system.

Workstation
An electronic computing device and the electronic media stored in its immediate environment.

III. POLICY

All employees, temporary staff, contractors, and consultants are required to read this policy and to sign an acknowledgement form verifying an understanding of the policy prior to using Dominion's corporate computing environment. All employees, temporary staff, contractors, and consultants must also have an understanding of the policies referenced at the end of this document. The Human Resources Department is responsible for communicating this policy and maintaining the signed acknowledgement forms.

Use of the corporate computing environment must be authorized prior to use, and may be monitored to verify authorized use, ongoing need, and adherence to security procedures. The use of the corporate computing environment constitutes consent to such monitoring, and users should have no expectation of privacy.

INFORMATION ACCESS

Access to computing facilities, and the information residing on computing facilities, must be limited to the level of access that is needed by an individual to perform his or her job functions. Individuals may not seek or be given access privileges beyond the reasonable minimum necessary access needed to perform their job function. This access is provided through a request process. The following specifications apply to Information Access:

1. **Minimal Access** – All Dominion employees are required to have basic system access to the Dominion computing environment. This access is to facilitate the required electronic submission of time sheets, basic correspondence within Dominion, and perform other work-related functions.
2. **Access Authorization** – All additional access requests beyond the minimal access must be approved by the appropriate personnel before the access can be granted. In addition, all access requests are to consider Segregation of Duties where appropriate and practical.

   To request new hire system access, the department manager will submit an access request form to the IT Department specifying the requested access. The IT Department will open a help desk ticket to document the access request and processing.
3. **Authority to Grant Access** – The user's manager and, in appropriate cases, the data owner (or delegate) approves access.
4. **User ID and Authentication** – Access to computing facilities and information must be controlled through the use of an individually owned unique user ID and associated confidential password or other approved authentication method. This password is used to authenticate the owner of the user ID and must never be shared with anyone.
   - The use of generic user IDs is not permitted. Management must approve System/Administrative/Operator type accounts. The IT Department will work with the appropriate users or system managers to gain the additional approvals for access. Example: Only system/operator type accounts can own system assets or processes.
   - The use of hardware or software to automatically provide access passwords, e.g. scripted passwords, is generally prohibited. In other words, the logon process may not be automated unless a legitimate need exists and has been approved through the exception process.
   - Network authentication must use a password that meets the requirements listed below.
     - The password must be at least eight (8) characters.
     - The password must contain at least one capital letter, at least one lower case letter, at least one number, and at least one special character.
     - The password must not contain the individual's user ID, or any part of the individual's name.
     - The password cannot be a password that the individual previously used.
     - The password should be a combination of upper and lower case letters.
     - The password expires after ninety (90) days.

5. **Access Controls** – When an individual's duties or employment status changes, management must submit a request to have his or her access privileges modified as required. For terminations, management must submit the request (i.e., access termination form) by the employee's last day of employment. For transfers, the current manager must submit a request to have all accesses that the employee no longer needs removed before the date of the transfer or before a specified time. The employee's new manager must submit a request to have the appropriate accesses given to the employee which are needed in his or her new job. Management must also review their staff's access privileges on a regular basis and submit access requests for any modifications that are required.
6. **Access Review –** The IT Department is tasked with the completion of regular access and role reviews on applications and platforms it deems appropriate. Business areas that support, utilize, or have data on these systems are required to support these reviews. The purpose of these reviews is to ensure that:
    - Processes are being followed and functioning properly.
    - Requests are receiving the appropriate authorizations.
    - Access rights are being granted appropriately.
    - Access rights are being modified or removed in a timely manner when they are no longer needed.
    - Access exceptions have a legitimate and ongoing business need.
    - Access is being used as granted.
7. **Usage** – Computer resources are to be used for business purposes only unless management has given appropriate approval.
    - They may not be used to harass others, degrade system performance, deprive access to a corporate resource, or gain access to a system or information for which proper authorization has not been given.
    - The unauthorized dissemination of PHI is not permitted.
    - The use of computing facilities in violation of local, state, and federal laws is prohibited.
    - Using or copying software in violation of license agreement or copyright laws is prohibited.
8. **Failure to Use Granted Access** – Granted computer access that is not used may be removed at the discretion of the IT Department, without notification. Internal applications access that is used less than once every 90 days may be deemed as no longer needed and considered appropriate for removal. In the event that the access is later required, access can be requested again through the formal request process.

WORKSTATION USE

All individuals are responsible for using computer resources in a professional, ethical, and lawful manner. All individuals are also responsible for protecting computer resources from unauthorized access.

Individuals must not leave computer system accounts open and accessible when they are not physically located at the workstation. The lock computer feature must be used to protect the workstation in order to prevent unauthorized access.

Individuals are not to store information locally (on their C: drive) or download software to their workstation that may have an effect on Dominion software and license compliance.

An individual who has been assigned a portable computing device, such as a laptop or personal digital assistant (PDA), must not leave the computing device unattended in public areas and must not permanently store protected health or other sensitive information on the device. If there is a business need and approved safeguards are installed and enabled on the device, then PHI or other sensitive information may be temporarily stored on the device.

DEVICE AND MEDIA CONTROL

PHI and other sensitive information must be removed from electronic media and/or devices when the asset or media is no longer needed and/or when the media will no longer be under corporate control. Examples would include, but not be limited to, media or devices that are retired, media or devices that are donated to charity, and any device that requires off site vendor maintenance or repair. The removal of this information must be followed by an approved overwrite operation using a data destruction utility specifically designed for this purpose. If this is not possible, the physical destruction of the media is required to insure the confidentiality of the information.

Storage or duplication of PHI or other corporate critical information on portable media should be performed only where there is a business need. Appropriate controls must be used to ensure the data is protected, such as encryption technology. Data placed on portable media must be logged and a copy retained. The storage or duplication of PHI or other corporate critical information on non-corporate, i.e. individually owned devices or media is not permitted.

VIRUS AND MALICIOUS SOFTWARE PROTECTION

All computing devices must utilize anti-virus and malware software where appropriate. The software must:

- Be enabled at all times.
- Scan for viruses and malware on a regular basis, in accordance with corporate guidelines.
- Have pattern files updated in accordance with corporate guidelines.

- Have on-access scanning enabled to ensure that any external files are scanned before being introduced into corporate computers.

E-MAIL AND THE INTERNET

Typically, e-mail and Internet facilities are to be used for business purposes only, unless management has given appropriate approval.

When using e-mail or the Internet you are acting as a representative of the company and must follow established policies. Adherence to the following is also required:

- E-mail and Internet connections are not to be used for personal gain or in support of any purpose not related to company business without management approval.

- The intentional interception, recording, reading, deletion, or reception of another individual's e-mail without proper authorization is not permitted.

- PHI and other sensitive information must not be sent outside the company unless it has been secured and is being sent to an authorized individual.

- Information that is attached to e-mail must be scanned for viruses before being introduced into, or before leaving, the corporate computing environment.

- Access to the Internet must pass through a controlled corporately recognized environment.

- Emails should not be stored in any location other than within the defined Dominion email solution. The use of .pst files or other means of archiving emails and data is not permitted.

- The sending, downloading, storing displaying, printing, or otherwise disseminating of material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or unlawful is not permitted. Please refer to the Code of Conduct for additional information.

REMOTE ACCESS

The only approved method of remotely accessing the corporate computing environment is through the use of the standard corporate solutions. Dominion's IT Strategy, for use by the IT Department, contains additional information about remote access.

The establishment of and or use of unauthorized remote access methods or technologies are expressly prohibited.

SECURITY AWARENESS

All existing members of the workforce are required to pass a Security Awareness training program, be aware of security policies, and understand the reasons why policies and procedures are in place. Workforce members must stay informed about their ongoing responsibilities, especially those related to securing PHI and other sensitive information.

REPORTING INCIDENTS

All users of Dominion's systems must report any unusual computer activity such as a perceived virus, an unauthorized access or use event, or loss or theft of Dominion equipment (e.g. laptop or mobile device), by submitting an IT Help Desk Ticket. In the event of loss or theft of Dominion equipment, the employee should also file a police report.

Further, disclosures of PHI should be reported to Dominion's Compliance/Privacy Office in accordance with the Guidelines When Filling Out Disclosure Forms.

The Privacy Officer will coordinate with IT, and vice versa, concerning information security and privacy matters.

VIOLATION OF POLICY

Individuals who suspect, or have knowledge of a violation of an information security policy must report that violation immediately to their manager/supervisor. The manager/supervisor should evaluate the information and contact IT Management if it appears that a violation has occurred. Reports can also be made to the Compliance Department or the Compliance Hotline.

Violation of this policy is subject to corrective action. Corrective action may start at any level, up to, and including, immediate termination depending on the severity of the violation.

Willful violation of applicable state and federal laws may also result in civil or criminal punishment as allowed by state and federal law.

EXCEPTIONS

The formal information security request process, i.e. submission of an access request, will govern any requests for exception to an information security policy to help ensure that all exceptions consider controls for PHI and other corporate sensitive information, while meeting the specific business requirements.

It is the responsibility of the information owner or access coordinator to ensure that an access request is completed to start the exception process and that the request includes the business need for the exception. The person assigned final security responsibility will evaluate the request and must approve all exception requests.

IV. RELATED INFORMATION/QUESTIONS

Please see the following for additional guidance:

- Capital BlueCross Code of Conduct (for internal use)
- Dominion National Code of Conduct (for external use)
- Dominion Information Security Strategy (for IT Department use)
- HR-0711, Building Security and Use of Facilities

- HR-0735, Privacy of Member Information
- HR-317, Involuntary Terminations
- PF-0301D, Record Retention and Destruction
- Guidelines When Filling Out Disclosure Forms

Questions related to protecting the confidentiality, integrity, and availability of protected heath information, and/or proprietary information, or any obligation under this policy should be directed to IT Management.

Questions regarding the administration of this policy may also be referred to the Human Resources Department.