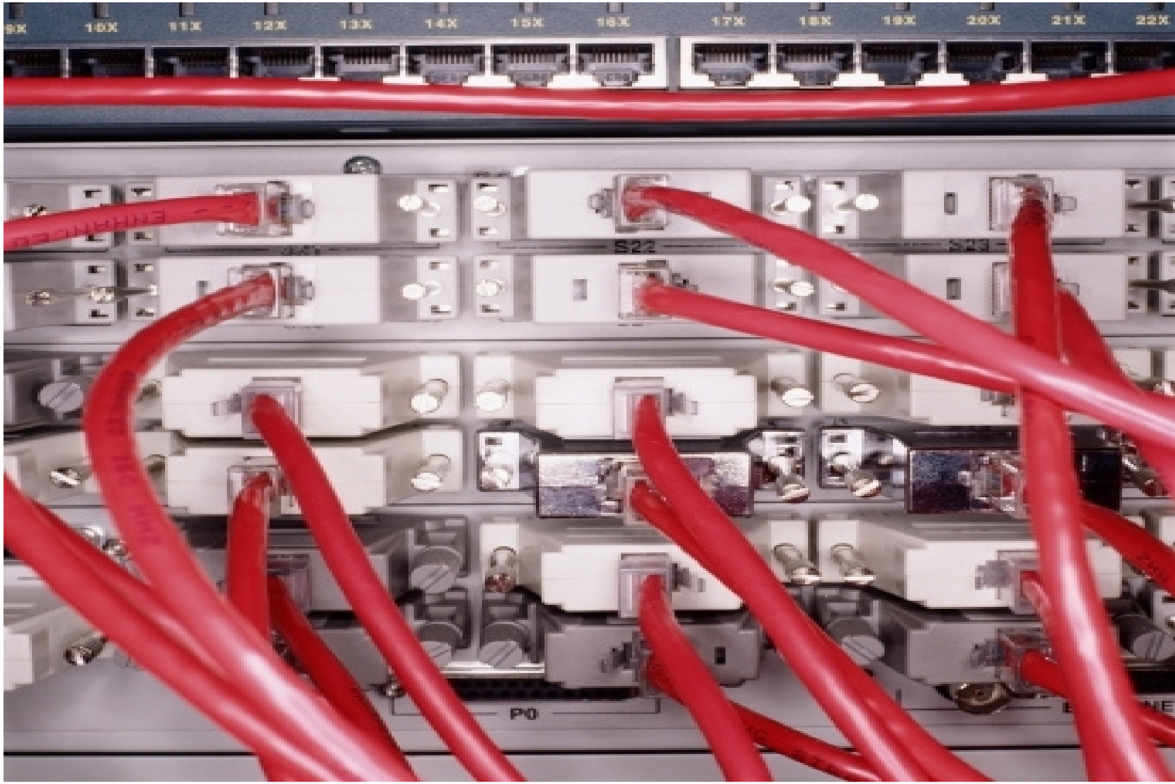
CATALYST
TECHNOLOGY GROUP
Innovating how IT is delivered.sm

Cyber Risk Assessment

Cyber Liability Questionnaire



CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

Table of Contents

Type Of Sensitive Data

Information Security Infrastructure And Organization

Does your company have an information security infrastructure and organization? Attach organizational charts or policy and procedure documents indicating the establishment of an information security infrastructure and organization.

Response
Yes

Responded By
Bruce Banner

Attached Images

Exhibits

- *KapDentalITInfrastructure.png*

Sensitive Data Checklist

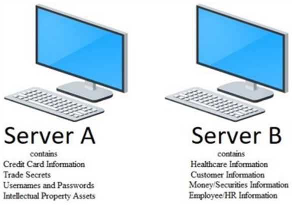
Do you collect, store, process and/or transmit any Sensitive Data on your computer system (check all that apply below)?

□	Credit Card Information
□	Healthcare Information
□	Trade Secrets
□	Customer Information (Names, Addresses, Email, Social Security Number)
□	Usernames and Passwords
□	Money/Securities Information
□	Intellectual Property Assets
□	Employee/HR Information

Responded By
Steve R

Additional Notes
Credit Card Information will be moved to different server in 2020.

Attached Images



Exhibits

- *serverSensitiveContents.png*

Total Number of Protected Records

Total number of protected records in your care, custody, or control:

Response
990

Maximum Number of Unique Individuals

Maximum number of unique individuals for whom you collect, store or process any personal information?

Response
99

Regulatory Or Compliance Frameworks Checklist

Is your company compliant with any of the following regulatory or compliance frameworks? (check all that apply and indicate most recent date of compliance)

Regulatory or Compliance Framework	Achieved Compliance	Most Recent Date of Compliance
ISO 17999	□	5/1/2019
SOX	□	
PCI-DSS	□	
HITECH	□	
HIPAA	□	
GLBA	□	
SSAE	□	
FISMA	□	

Industry Security Frameworks

Does your company leverage any industry security frameworks for confidentiality, integrity and availability (e.g., NIST, COBIT)?

Response
No

Outside Security or Privacy Groups

Is your company an active member in outside security or privacy groups (e.g., ISAC, IAPP, ISACA)?

Response
No

Sensitive Data Processed

Is any Sensitive Data processed, stored, inputted, collected or otherwise handled on or in any of the following assets under your control or authorization?

□	Websites
□	Computer Systems
□	Laptops, personal portable or mobile devices
□	Physical files and premises

Sensitive Information in Custody

Do you know what sensitive or private information is in your custody along with whose info it is, where it is, and how to contact those individuals if their information is breached?

Response
No

Total Global IT Budget Allocated to Security?

What percentage of your total global IT budget is allocated to security?

Response
10%

Third Parties

Percentage of Work Subcontracted to Others

What percentage of the Applicant's business involves subcontracting work to others?

Response 10%

Evidence of Errors and Omissions Insurance from Subcontractors

Does the Applicant require evidence of the errors and omissions insurance from subcontractors? (Please attach copies of evidence of errors and insurance)

Response Yes
Attached Images
Exhibits ● *KapDentalErrorsAndOmissionsInsurance.docx*

Written Contracts with Clients

Does the Applicant use a written contract with clients? (Please attach copies of written contracts)

Response Yes
Attached Images
Exhibits ● *CustomerContract.docx*

Contracts Review Prior to Use

Does an attorney review such contracts prior to use?

Third Parties

Percentage of Work Subcontracted to Others

What percentage of the Applicant's business involves subcontracting work to others?

Response
10%

Evidence of Errors and Omissions Insurance from Subcontractors

Does the Applicant require evidence of the errors and omissions insurance from subcontractors? (Please attach copies of evidence of errors and insurance)

Response
Yes

Attached Images

Exhibits

- *KapDentalErrorsAndOmissionsInsurance.docx*

Written Contracts with Clients

Does the Applicant use a written contract with clients? (Please attach copies of written contracts)

Response
Yes

Attached Images

Exhibits

- *CustomerContract.docx*

Contracts Review Prior to Use

Does an attorney review such contracts prior to use?

Response
Yes

Hold Harmless Clauses

Does the standard contract contain hold harmless clauses for the benefit of the Applicant?

Response
Yes

Consent to Hold Harmless/Indemnify Others

Does the Applicant agree to hold harmless/indemnify others?

Response
Yes

Company Information Responsible Individual

Is there an individual responsible for the security of the company information that resides at third party technology service providers?

Response
Yes

Follow-up: Company Information Responsible Individual

Responsible Individual

Enter the name of the responsible individual:

Response
Steve Rogers

Payment Processing

Do you process payments on behalf of others, including eCommerce transactions?

Response
Yes

Protected Personal Information or Protected Healthcare Information

Do you collect, input, store, process, or maintain any Protected Personal Information or Protected Healthcare Information Records for third party corporate entities?

Response
Yes

Third Party Corporate Confidential Information

Do you store, process or maintain any third party corporate confidential information?

Response
Yes

Information Sharing

Does the Applicant share private or personal information gathered from customers (by the Applicant or others) with third parties?

Response
Yes

Information Security Staff

Do you outsource your information security to a firm specializing in information security or have staff responsible for and trained in information security?

Response
Yes

Follow-up: Information Security Staff

List of Information Security Staff

Enter the name of firm or staff member(s):

Response
Compu-Global-Hyper-Mega-Net

Network, Computer System, Information Security Outsourcing

Do you outsource any part of your network, computer system or information security functions?

Response
Yes

Follow-up: Network, Computer System, Information Security Outsourcing

Outsourced Security Services

Indicate which services are being provided and the vendor's name:

Service	Outsourced	Vendor Name
Data Center Hosting	□	Compu-Global-Hyper-Mega-Net
Managed Security	□	
Data Processing	□	
Application Service Provider	□	
Alert Log Monitoring	□	
Offsite Backup and Storage	□	

Cloud Service Providers

Does the Applicant currently use a Cloud Service Provider in the course of business operations?

Response
Yes

Follow-up: Cloud Service Providers

List of Cloud Service Providers

List all Cloud Service Providers.

Response
SHIELD

Do you require third party technology providers meet required regulatory requirements (e.g., PCI-DSS, HIPAA, SOX, etc.)?

Response
N/A

Third Party Security Provisions

Do third party contracts include security provisions? Attach contracts or portions related to security provisions.

Response Yes
Attached Images
Exhibits ● *KapDentalSecurityProvisions.docx*

Third Party Security Standards

Does your company enforce security standards for third parties that connect to your network?

Response Yes

Third Party Security Assessments or Audits

Does your company perform assessments or audits to ensure third party technology providers meet company security requirements?

Response No

Contract Review and Approval Process

Does your company have a formal process for reviewing and approving contracts with third party technology service providers? Please attach appropriate documentation.

Response Yes

Sensitive or Confidential Information Written Agreements

Do you enter into written agreement for such third-party services that address care, use, and control of sensitive or confidential information?

Response
No

Hold Harmless and Indemnification Agreements

Do contracts with service providers include hold harmless and indemnification agreements? Attach agreements or relevant sections.

Response
Yes

Attached Images

Exhibits

- *KapDentalHoldHarmlessContracts.docx*

Data Protection Reviews

Does the company perform reviews at least annually of the company's third-party service providers to ensure they adhere to company requirements for data protection?

Response
No

Vendor Liability Insurance

Does your company require all vendors to maintain liability insurance? Attach Policy and Procedures and indicate relevant section in notes.

Response
Yes

Evidence of Network Security and Privacy Liability Coverage

Do you require third parties to provide evidence of network security and privacy liability coverage? If yes, please note where those records are kept.

Response
Yes

Computer Service Provider Security Policies and Procedures

Do you require computer service providers who may have access to confidential information or PII to demonstrate adequate security policies and procedures?

Response
No

Healthcare Information Exchanges

If the Applicant is in the healthcare industry, does the Applicant host, operate or manage a Healthcare Information Exchange on which other organizations may store PHI?

Response
Applicant does not operate or manage a Healthcare Information Exchange

Vendor Data Security

Do you require all vendors to whom you outsource data processing or hosting functions (e.g., data backup, application service providers, etc.) to demonstrate adequate security of their computer systems?

Response
Yes

Follow-up: Vendor Data Security

Method of Verification

Please indicate method of verification:

Response
Security is assessed by internal staff

Third Party Audit or Monitoring

Have the Applicant's internal networks and/or Computer Systems been subject to third party audit or monitoring?

Response
Yes

Follow-up: Third Party Audit or Monitoring

Date of Last Audit and List of Improvements and Recommendations

When was the last audit? Attach list of improvements and recommendations.

Response 4/30/19
Attached Images
Exhibits ● *KapDentalImprovements.docx*

Follow-up: Third Party Audit or Monitoring

Improvements and Recommendations Implementation

Have all improvements and recommendations been implemented? Attach relevant documentation.

Response Yes
Attached Images
Exhibits ● *KapDentalImprovementsCompleted.docx*

Handling of Data

Sensitive Data Management Process

Do you have a process to manage access to Sensitive Data including timely account termination?

Response
Yes

Follow-up: Sensitive Data Management Process

Sensitive Data Management Process Details

Please describe:

Response
Erase terminated employee accounts completely.

Former Employee Associated Computer Access Termination

Is all associated computer access terminated when an employee leaves the company?

Response
Yes

User Account Processes

Does the company have processes established that ensure the proper addition, deletion and modification of user accounts and associated access rights?

Response
Yes

User Account Management Process

Does your company have a process for managing user accounts?

Response
Yes

Firewall

Does the Applicant have up-to-date, active firewall technology?

Response
Yes

Follow-up: Firewall

Firewall Vendor

Which firewall vendor is used?

Response
ZoneAlarm

Follow-up: Firewall

Firewall Update Procedure

What is the current procedure for updating the firewall?

Response
Steve updates it daily.

Anti-virus

Does the Applicant currently have in place updated anti-virus software active?

Response
Yes

Anti-virus Installation

Is anti-virus installed on all of the Applicant's computer systems, including laptops, personal computers and networks?

Response
Yes

External Computer System Intrusion Prevention

Do your external computer systems (e.g., commercial websites and mobile devices) use firewall and intrusion prevention systems?

Response
Yes

Follow-up: External Computer System Intrusion Prevention

Intrusion Prevention Security Technologies

Please identify the security technologies used:

Response
ZoneAlarm

Password Management Process

Does your company enforce a password management process?

Response

Password Complexity

Does the company enforce passwords that are at least seven characters and contain both numeric and alphabetic characters?

Response
Yes

Password Expiration

Are procedures in place regarding the creation and periodic updating of passwords?

Response
Yes

User and Password Procedure Documentation

Does the Applicant have a formal documented user and password procedure in place? Attach documentation.

Response

Yes

Multi-Factor Login

Does Applicant currently have in place Multi-Factor login for privileged access? Attach documentation or screenshots.

Response
Yes

Critical System Security Testing

Do critical systems receive full security testing before deployment? Attach proof of latest tests.

Response
Yes

System Security Considerations

When a new system is developed or purchased, are security considerations taken into account? Attach relevant procedures document.

Response
Yes

Production Security Review

Are new applications and non-cosmetic changes reviewed for security vulnerabilities prior to migration to production? Attach relevant procedures document.

Response
Yes

Separation of Development Systems

Are staging, test, and development systems kept separate from production systems? Attach network diagram indicating the separation of staging, test, development, and production systems.

Response
Yes

Technical Security Configuration Documentation

Is there technical security configuration documentation for the technologies or major business applications in your company?

Response
Yes

Follow-up: Technical Security Configuration Documentation

Technical Security Configuration Documentation Location

Where is the documentation stored?

Response
C:\ on main computer

Security Products

Does your computer system (including e-mail and remote access) use security products that address viruses, worms, Trojans and other malware?

Response
Yes

Follow-up: Security Products

Security Products Used

Please identify the technologies used:

Response
GFI Languard
GFI Software VIPRE
Microsoft Security Essentials
Symantec AntiVirus
VIPRE
Windows Defender

Virus Controls and Filtering

Do you implement virus controls and filtering on all systems?

Response
Yes

Anti-virus and Firewall Updates

Do you have anti-virus software and firewalls in place that are regularly updated (at least quarterly)?

Response
Yes

Anti-malware

Does the company install and update an anti-malware solution on all systems commonly affected by malicious software (particularly personal computers and servers)?

Response
Yes

Retired Software or Hardware

Does the company use any software or hardware that has been officially retired (i.e., considered 'end- of-life') by the manufacturer (e.g., Windows XP)?

Response
Yes

Critical Patches

Are critical patches installed within thirty (30) days of release?

Response
Yes

Physical Security

Do you have physical security program in place to prohibit and track unauthorized access to your computer system and data center?

Response
Yes

Follow-up: Physical Security

Physical Security Program Details

Please describe the physical security program. Attach additional documentation if available.

Response We have security guards at every entrance and exit.
Attached Images
Exhibits ● *KapDentalSecurityGuardFloorPlan.docx*

Automated Patch Management

Do you have an automated patch management program?

Response Yes

Unauthorized Access

Do you have a way to detect unauthorized access or attempts to access sensitive information?

Response Yes

Follow-up: Unauthorized Access

Unauthorized Access Detection Details

Please describe how you detect unauthorized access or attempts to access sensitive information.

Response Steve checks logs daily.

Intrusion Detection

Does the company have an intrusion detection solution that detects and alerts an individual or group responsible for reviewing malicious activity on the company network?

Response
Yes

Follow-up: Intrusion Detection

Intrusion Detection Software

What intrusion detection software are you using?

Response
McAfee

Security Software Upgrades

Describe the process for upgrading security software (i.e. how often and by whom):

Response
Steve updates it every day.

Physical Access

Does the company have entry controls that limit and monitor physical access to company facilities (e.g., offices, data centers, etc.)? Attach photos of entry controls.

Response
Yes

Attached Images

Exhibits

- *KapDentalSecurityPlan.png*

Network Changes

Do you control and track all changes to your network to ensure that it remains secure?

Response
Yes

Follow-up: Network Changes

Network Change Tracking

How are changes tracked?

Response
Steve keeps logs.

Network Security Controls

Do you have a procedure to test or audit network security controls?

Response
Yes

Follow-up: Network Security Controls

Network Security Controls Details

Please describe. Attach additional documents if available.

Response

Attached Images

Exhibits

- *Network Security Controls Details.docx*

Internet/DMZ Systems

Are systems in your Internet/DMZ environment secured?

Response
Yes

Internal Systems

Are internal systems secured?

Response
Yes

Network Access Controls

Are controls in place to secure network access?

Response
Yes

Follow-up: Network Access Controls

Network Access Controls Details

Please describe. Attach additional documents if available.

Response
see docx

Attached Images

Exhibits

- *Network Access Controls Details.docx*

Open Source Software Updates

Does the company update open source software (e.g., Java, Linux, PHP, Python, OpenSSL) that is not commercially supported for known security vulnerabilities?

Response
Yes

Follow-up: Open Source Software Updates

Open Source Software Updates Details

Please describe. Attach additional documents if available.

Response
see docx

Attached Images

Exhibits

- *Open Source Software Updates Details.docx*

Factory Default Settings

Do you replace factory default settings to ensure your information security systems are securely configured?

Response
Yes

Vulnerability Assessment

Do you have a proactive vulnerability assessment program that monitors for breaches and ensures timely updates of anti-virus signatures and critical security patches?

Response
Yes

Virus Signatures

How often are virus signatures updated?

Response
daily

Patch Management Procedures

Does the Applicant currently have in place patch management procedures?

Response
Yes

Commercial Software Updates

Does the company update (e.g., patch, upgrade) commercial software for known security vulnerabilities per the manufacturer advice?

Response
Yes

Multi-Factor Authentication

Does the company use multi-factor authentication for remote network access originating from outside the company network by employees and third parties (e.g., VPN, remote desktop)?

Response
Yes

Follow-up: Multi-Factor Authentication

Multi-Factor Authentication Details

Please describe. Attach additional documents if available.

Response
email and phone number verification

Attached Images

Exhibits

- *Multi-Factor Authentication Details.docx*

Remote Access

Does the Applicant currently have in place remote access limited to VPN?

Response
Yes

Mobile Device Unauthorized Access

Does the company have a solution to protect mobile devices (e.g., Laptops, iPhones, iPads, Android, Tablets) to prevent unauthorized access in the event the device is lost or stolen?

Response
Yes

Follow-up: Mobile Device Unauthorized Access

Mobile Device Unauthorized Access Solution Details

Please describe. Attach additional documents if available.

Response
we erase them remotely

Attached Images

Exhibits

- *Mobile Device Unauthorized Access Solution Details.docx*

Laptop or Web Server Sensitive Data

Does the Applicant store sensitive data on laptops or web servers?

Response
Yes

Follow-up: Laptop or Web Server Sensitive Data

Laptop or Web Server Sensitive Data Encryption

Is the data encrypted?

Response
Yes

Encryption Tools

Do you have encryption tools to ensure integrity and confidentiality of Sensitive Data including data on removable media (e.g., CDs, DVD, tapes, disk drives, USB devices etc.)? If 'Yes', please describe technologies used:

Response
Yes

Follow-up: Encryption Tools

Encryption Tools Details

Please describe technologies used. Attach additional documents if available.

Response
see docx

Attached Images

Exhibits

- *Encryption Tools Details.docx*

List of Encrypted Privacy Information

Does your company encrypt Privacy Information when: (Check all that apply)

□	Data is at rest
□	Transmitted over public networks (e.g. the Internet), in transit
□	Stored on mobile assets (e.g. laptops, phones, tablets, flash drives)
□	Stored on enterprise assets (e.g. databases, file shares, backups)
□	Stored with 3rd party services (e.g. cloud)

Portable Data Storage

Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?

Response
Yes

Portable Data Storage Security

Describe any additional controls the Applicant has implemented to protect data stored on portable devices:

Response
Remote data deletion.

Portable Data Storage Encryption

Are tapes and other portable media containing backup materials encrypted?

Response
Yes

Offsite Portable Data Storage Secure Transportation and Facilities

Are tapes or other portable media stored offsite using secured transportation and secured facilities?

Response
Yes

Offsite Portable Data Storage Transportation Logs

If stored offsite, are transportation logs maintained?

Response
Yes

Onsite Portable Data Storage Physical Security Controls

If stored onsite, please describe physical security controls

Response
Yes

Remote Access Encryption

Do you authenticate and encrypt all remote access to your network and require all such access to be from systems at least as secure as your own? Check N/A if you do not allow remote access to your systems.

Response
Yes

Wireless Network Security

On your wireless networks, do you use security at least as strong as WPA authentication and encryption? Check N/A if you do not use wireless networks.

Response
Yes

External Network Privacy Information Security

Does your company store Privacy Information on a secure network zone that is segmented from internal network?

Response
Yes

Configuration Management

Does your company perform configuration management?

Response
Yes

System Logs

Do you maintain system logs?

Response
Yes

System Log Security Review

Are system logs reviewed for security related events?

Response
Yes

System Log Review Frequency

Are system logs reviewed daily, weekly, monthly?

Response
Daily

Network Change Tracking

Do you control and track all changes to your network to ensure that it remains secure?

Response
Yes

Credit Card Transactions

Do you process, store, or handle credit card transactions?

Response
Yes

Follow-up: Credit Card Transactions

PCI DSS Compliance

Are you compliant with Payment Card Industry Data Security Standards (PCI DSS)?

Response
Yes

Website Sensitive Data

Do your Websites use Sensitive Data?

Response
Yes

Follow-up: Website Sensitive Data

PCI DSS Compliance

Are you compliant with Payment Card Industry Data Security Standards (PCI DSS)?

Response
Yes

Follow-up: PCI DSS Compliance

Evidence of PCI DSS Compliance

Were you found to be in compliance? Upload latest findings.

Response
Yes

Attached Images

Exhibits

- *Evidence of PCI DSS Compliance.docx*

Policies, Procedures and Documentation

Policies and Procedures Implementation

Do you implement policies and procedures to ensure compliance with legislative, regulatory and/or contractual privacy requirements that govern your industry?

Response
Yes

Risk Management Procedures

Does the Applicant have any risk management procedures in place (please attach a copy of procedures)?

Response
Yes

Privacy Information Storage and Transmission Documentation

Does the company maintain documentation that clearly identifies the storage and transmission of all Privacy Information?

Response
Yes

Third Party Information Sharing Privacy Policy

Does your privacy policy allow you to share information with third parties?

Response
Yes

Follow-up: Third Party Information Sharing Privacy Policy

Vendor Contracts

Do your contracts with vendors and others with whom you share or store Sensitive Data require the other party to defend and indemnify you for legal liability arising from any release or disclosure of the information due to the negligence of the vendor or other party?

Response

Yes

Business Continuity Plan and Disaster Recovery Plan

Does your organization have a Business Continuity (BCP) and Disaster Recovery (DR) plan?

Response
Yes

Business Continuity/Disaster Recovery Plan Testing

Was your Business Continuity/Disaster Recovery Plan tested during the past year or how often is it tested?

Response
Yes

Expected Downtime for Critical Business Systems

What is the greatest expected downtime (in hours) for critical business systems?

Response
1 hr

Operations Restoration Time

How long does it take to restore your operations after a computer attack or other loss/corruption of data?

Response
12 hrs or less

Security Incident Response Plan

Do you have a security incident response plan in case of a security breach?

Response
Yes

Follow-up: Security Incident Response Plan

Security Incident Response Plan Alternative Options

Does your security incident response plan include alternative options to account for incapacitated third-party outsourcing providers which you depend on?

Response
Yes

Follow-up: Security Incident Response Plan Alternative Options

Security Incident Response Plan Alternative Option Details

If "Yes," explain:

Response
We have backup servers.

Company Property Security and Acceptable Use Policy

Do you have a company policy governing security and acceptable use of company property?

Response
Yes

Computer Use Policies

Does the Applicant have computer use policies?

Response
Yes

Computer Security Policy

Does the Applicant have a computer security policy?

Response
Yes

Laptop Security Policy

Does the Applicant maintain a laptop security policy?

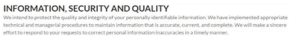
Response
Yes

Information Security Policy and Privacy Policy

Do you have a comprehensive Information Security Policy and Privacy Policy that is updated and enforced on continual basis? Attach a copy of the privacy policy.

Response
Yes

Attached Images



INFORMATION, SECURITY AND QUALITY
We intend to protect the quality and integrity of your personally identifiable information. We have implemented appropriate technical and managerial procedures to maintain information that is accurate, current, and complete. We will make a sincere effort to respond to your requests to correct personal information inaccuracies in a timely manner.

Exhibits
- *privacyPolicy.png*

Follow-up: Information Security Policy and Privacy Policy

Privacy Policy Review

Has your Privacy Policy been reviewed by a qualified attorney?

Response
Yes

Follow-up: Privacy Policy Review

Privacy Policy Review Attorney Name

Enter the name of the qualified attorney:

Response
Bruce Wayne

Privacy Policy Compliance

Is the Applicant in compliance with its privacy policy?

Response
Yes

Privacy Policy Author

Who developed the privacy policy? Internally developed or third party?

Response
Third Party

Follow-up: Privacy Policy Author

Privacy Policy Third Party Author

Name of third party:

Response
Scott Lang

Privacy Policy Last Review Date

When was the company's privacy policy last reviewed?

Response
4/29/19

Privacy Policy Review and Update Frequency

How often is it reviewed and updated?

Response
Monthly

Identity Theft Prevention Program

Have you implemented an identity theft prevention program (aka FTC "Red Flags" program)?

Response
Yes

Chief Information Officer

Does the Applicant employ a Chief Information Officer?

Response
Yes

Follow-up: Chief Information Officer

Chief Information Officer Name

Name of CIO:

Response
Diana Prince

Chief Security Officer

Do you have a Chief Security Officer (CSO) or equivalent?

Response
Yes

Follow-up: Chief Security Officer

Chief Security Officer Name

Name of CSO:

Response
Joe Cool

Supervisor of CSO or Security Policy Management and Compliance Position(s)

To what position within the organization does this person report?

Response
Charlie Brown

Chief Privacy Officer

Do you employ a chief privacy officer or an equivalent?

Response
Yes

Follow-up: Chief Privacy Officer

Chief Privacy Officer Name

Name of chief privacy officer:

Response
Clark Kent

Website Privacy Disclosure Statement

Do you have a privacy disclosure statement on your website?

Response
Yes

Follow-up: Website Privacy Disclosure Statement

Website Privacy Disclosure Statement URL

URL to privacy disclosure statement:

Response
http://kaplandentalsuperfundentistry.com/privacy.html

Secondary/Backup Computer System

Does the Applicant have a secondary/backup computer system?

Response
Yes

Follow-up: Secondary/Backup Computer System

Secondary/Backup Computer System Restore Time

If secondary/backup system is in place, how long before this system is operational?

Response
1h

Sensitive Data Backup and Restore Methodology

Do you have a backup and restore methodology for your sensitive data?

Response
Yes

Computer System and Data Back-ups Schedule

Do you run computer system and data back-ups on a regular basis?

Response
Yes

Daily Valuable/Sensitive Data Backups

Is valuable/sensitive data backed-up by Applicant on a daily basis?

Response
Yes

Weekly Valuable/Sensitive Data Backups

Is valuable/sensitive data backed-up by Applicant at least once a week?

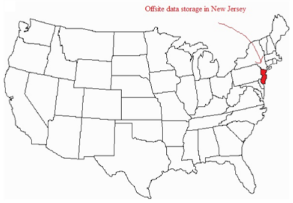
Response
Yes

Off-site Valuable/Sensitive Data Storage

Do you secure such data to an off-site storage location?

Response
Yes

Attached Images



Exhibits

- *offsiteDataStorage.png*

Complete Back-up File Generation Secure Offsite Storage

Is at least one complete back-up file generation stored and secured offsite separate from the Applicant's main operations in a restricted area?

Response
Yes

Backup and Storage Format

What format do you utilize for backing up and storage of computer system data--tape or other media, online backup service, or other?

Response
online backup service

Document Retention and Destruction Policy

Do you have a document retention and destruction policy within your organization?

Response
Yes

Mobile Device Encryption Policy

Do you have a written policy which requires that PII stored on mobile devices (e.g. laptop computers/ smartphones) and portable media (e.g. flash drives, back-up tapes) be protected by encryption? Attach policy.

Response
Yes

Communication Encryption Policy

Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted?

Response
Yes

Compliant Procedure

Does the Applicant have a procedure requiring the review or follow-up of complaints?

Response
Yes

Access Control Procedures

Do your company's access control procedures address access to sensitive systems, files and directories? Attach and reference procedures.

Response
Yes

Data Classification Scheme

Do your company's policies address access to data based on a data classification scheme?

Response
Yes

Employees

Employee Access to PII Restriction

Do you restrict employee access to PII on a business-need to know basis?

Response
Yes

Restricted Employee Access to Private Information

Does the Applicant have restricted employee access to private information?

Response
Yes

New Hires Formalized Training Program

Does the Applicant have a formalized training program for newly hired employees?

Response
Yes

Data Privacy and Security Awareness Training

Do you provide awareness training for employees on data privacy and security including legal liability issues, social engineering issues (e.g., phishing), spam, dumpster diving, etc.? Attach presentation or note training methodology.

Response
Yes

Follow-up: Data Privacy and Security Awareness Training

Data Privacy and Security Awareness Training Medium and Frequency

If "Yes," please describe the medium and frequency of training:

Response
Steve provides the training monthly.

Security Issues and Procedures Employee Training

Is employee training conducted regarding security issues and procedures?

Response
Yes

Security Awareness Training

At least once a year, do you provide security awareness training for everyone who accesses your network?

Response
Yes

Employee Computer and Information Systems Policies and Procedures

Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees?

Response
Yes

Annual Employee Training and Certification

Do you provide annual employee training and certification?

Response
Yes

Annual Security Awareness Training

Does the company require annual security awareness training for all personnel so they are aware of their responsibilities for protecting company information and systems?

Response
Yes

Employee Personal Liability

Are employees aware of their personal liability and any potential ramifications if they aid, abet, or participate in a data breach incident involving the organization?

Response
Yes

Employee Screening

Does the company screen potential personnel prior to hire (e.g., background checks include previous employment history, drug, criminal record, credit history and reference checks)?

Response
Yes

Applicant's Hiring Process Checklist

In all cases, does the Applicant's hiring process include the following? (please check all that apply)

□	Criminal Convictions
□	Educational Background
□	Credit Check
□	Drug Testing
□	Work History