Business Continuity Plan

Coastal Veterinary Clinic

Sharyl Lynn Riley

December 16, 2020

Business Continuity Plan for Coastal Veterinary Clinic

Executive Summary

A Business Continuity Plan is designed to prepare an organization to cope with the various levels of emergencies. When relocating to a new site, management needs to protect the business from an unplanned situation that may exist during relocation. The purpose of this document provides a Business Continuity Plan for Coastal Veterinary Clinic on their alternative site operation.

Introduction

This document contains a BCP for Coastal Veterinary Clinic. It includes the information required for decision making and the agency response to any disaster, relocation to another site as well as the budget for the alternative worksites. This Coastal Veterinary Clinic BCP must be kept current to maintain the precision of its content. All individual assigned for information and material of its content must be committed to maintaining and updating details.
Although the plan is intended to provide guidance on budgeting, emergency response, risk management, recovery plan, and relocation, it shouldn't be used as a criterion for informed decision making.

The Objective of the Plan

This plan aims at providing a flexible response so that Coastal Veterinary Clinic can;

- Effectively relocate the business
- Response to destructive incidents
- Maintain operation during an episode
- Return to normal/usual activities (recovery)

Business Continuity Requirements

During relocation, activation of the business is always the main task. Equipment, software, hardware, human resources need to be intact for effective operation. The activation process in a new site would require the following;

- Inventory of all hardware, software, storage, server, and networking devices
- Checking of current equipment
- Computer networking and telephone disruption procedure as well as their recovery
- Provision of all critical records including both paper and electronic for patients, supplies, and certification.

Continuity and Recovery

Following the relocation of the business to an alternative site, the decision will be made according to the damage assessment, emergency response, and the nature of severity of the disruption. In case the department experiences a severe loss like loss of staff and hazardous environmental response the incident commander with the consultation of the clinic leadership will seek the way forward.

- Initial actions were taken during continuity
- Inform all staff on the BCP updates
- Documentation of major equipment as well as suppliers
- Staff assessment and documentation
- Communication departments' needs and status.

- Assessment of essential staffing needs and the estimated staffing needs.
- Implementation of Alternative staffing strategies

Cooperate service management

Each department would require a corporate service for operation. Department roles and responsibility will be vital for the normal resumption of duties. Power is a major expense and resource at any animal clinic. The organization will provide an emergency generator for critical outlets in animal care. During daytime, the clinic will ensure maximum utilization of daylight by opening curtains as well as the use of drapes. On the event of damage or malfunction of the generator, the technical department will use large power batteries till the issue is resolved. At the new location, the company will obtain bottled water form external distributes and adopt a waterless hand cleaning where possible.

Alternative location issues

Coastal Veterinary Clinic will be relocated to the alternative site as identified in the BCP. Due to the anticipated challenges, various staff members might be assigned extra roles. In the event where the anticipated location is unsafe for the clinic operations, the management will initiate closure and procedure for identifying a new site activated. Conditions considered for a new location include security, electricity, temperature control, the ability to house dogs and cats, emergency services, and water.

Recovery and resumption of all services

Before moving to normal procedures, recovery phase is important in determining the state of equipment, facilities, and resources. After the confirmation, Coastal Veterinary Clinic can

resume their normal operations at the new site. The manager will perform the following activities to ensure recovery and resumption of the business;

- Confirm that all staff are available at the new site
- Assign staff new rules
- Notify suppliers of the relocation
- Request the IT and communication department submit their necessities
- Determine inventory, clinical care, and hardware equipment.
- Notify agencies and stakeholders of reopening.

Estimated monthly Budget

Monthly Expenses	**Budget ($)**
Rent	5,000
Insurance	2,000
Networking and Communication	1,000
Maintenance expense	1,000
Utilities	500
Janitorial Service	1,500
Property Taxes	1,000
Total Monthly Costs	**12,000**

Relocation Costs

Expense	**Budget**
Architect/space planning	5,000
Attorney cost	3,000
Communication and Network consultation	4,000
Additional Tenant Upgrading, Not Counted in Rent	5,000

Security Deposit	1,000
Security System, Door Locks, and Alarms	5,000
Network and communication cabling	5,000
New Equipment/Furnishing Expenses	15,000
Office Equipment, Copiers, Fax Machines,	20,000
Furnishings	10,000
Animal Housing and Storage	10,000
Inspection	1,000
Public Advertisement of the relocation	10,000
Total Relocation Cost	**94,000**

DISASTER RECOVERY PLAN

A critical part of Coastal Veterinary Clinic's infrastructural deployment within an IT-based environment is the disaster recovery plan. When we think of IT management and business continuity, disasters generally incorporate risks of service outage while business is being conducted which could be caused by software, hardware, or generally a failure in the environment and the necessary process of controlling that outage. The purpose of the disaster recovery plan policy is to prepare Coastal Veterinary Clinic in the unfortunate instance of disruptions affecting the LAN, WAN, Internet access, and wireless network services due to natural disasters or man-made events. The plan will guide the restoration of network integrity and normal operations in the shortest possible time frame. Finally, providing an explanation of the selected DRP accomplishes these goals.

The Disaster Recovery Plan Policy would cover the use of all information, the IT equipment and security within an organization. The DRP will always encompass email, voice, internet, and mobile IT equipment. Within Coastal Veterinary Clinic the policy must be applied to all Doctors

and employees within the clinic. Despite efforts sometimes to recover the servers only partial restoration is achieved for data files while the server itself remains down. To avoid the recurrence of this problem, changes must be made on the back up procedure to establish a more stable restoration process. If the assessment of any disruption indicates an extended outage, the DRP would come online after the approval of the Disaster Recovery Team.

Network Architecture

The Disaster Recovery Team is responsible for making the declaration of disaster and for activating the recovery teams. The Disaster Recovery Team consist of the following personnel: Doctor Dog, Doctor Cat and the IT Manager. The Clinic is smaller and consists of two Doctors (owners) and 8 employees including the IT Manager. As a result, the Disaster Recovery Team is the same as the emergency management team. Assessment - the critical operations of the clinic, the following may be affected:

- Legal & Regulatory compliance
- Safeguarding sensitive company data
- Safeguarding sensitive client information
- Payment services
- Production of requirements

In the animal health insurance industry, medical benefits, premiums costs and customer information are regularly updated, internally and externally, by different methods remotely or on the clinic's network, by the clinic's employees and/or the actual customers. Due to the extreme need to keep this critical data confidential and protected, methods on use, sharing,

storing and protecting this data from unintentional disclosure requires extra care during an outage and a clear disaster recovery plan policy.

The objective is to ensure the survival of the clinic by establishing a culture that will identify and manage the risks that could cause the clinic to suffer. Some of the risks involved due to a disaster include the following:

- Failure to maintain critical customer services
- Failure to protect the company assets
- Damage to the company reputation
- Business control failure
- Failure to meet legal requirements

Scenarios

In the event of a natural disaster affecting Coastal Veterinary Clinic's network operations, Doctor Dog and Doctor Cat should be immediately notified.

If the disaster can be tracked within 48 hours, the following should be done:

- Portable generators with fuel should be deployed
- Network technical and admin personnel should be on standby
- Facilities department should be on standby for replacement shelters

If the potential disaster can be tracked 24 hours prior, then:

- Images of the network and system databases, along with other relevant files should be created
- Critical network and system elements should be backed up

- Verify the backup generator fuel status and operation
- Backups of routers, email, switches, and file servers
- Emergency trailers and fuel vehicles

In the event of a network outage, Doctor Dog, Doctor Cat and the IT Manager should be notified first to determine the cause of the outage and the timeframe for recovery. If the outage looks to be greater than an hour, all calls should be routed through alternate services.

Incident Response Team Charter

Executive Summary

The charter declares the organization's Incident Response Team (IRT) as the core management group responsible for responding to the loss of sensitive company information. The objective of the incident response plan is to define and implement an operational framework including the skills, processes, and tools need to recover from incidents impacting the networks and sensitive company data. The plan defines the incident management team, roles, and responsibilities and establishes practices for a timely recovery. Doctor Dog, Doctor Cat and the IT Manager make up the IRT.

Mission Statement

The mission of the Coastal Veterinary Clinic IRT is to mitigate the risk associated with the loss of the clinic network and sensitive data pertaining to the operations, employees, and clients and to oversee response efforts to the incidents. The IRT will play a vital role in protecting the brand and mission of Coastal Veterinary Clinic along with maintain trust between the Coastal Veterinary Clinic and its clients. The mission will be to ensure the following:

- Effective procedures are carried out for identifying actual breaches
- Overseeing the departmental response efforts regarding sensitive company data
- Implement security solutions to mitigate the potential loss of data
- Monitor the environment to raise awareness of threats to the department

Incident Declaration

Privacy incidents that may fall outside of the scope of the clinic's IRT may include incidents classified as a breach of sensitive clinic information. A privacy incident may be governed by regulations such as the Occupational Safety and Health Administration (OSHA). The loss of control of sensitive information may result from loss or theft of devices, loss of documents, human error, or the exploitation using technology. Details of an incident may come from various sources such as monitoring software, a reported loss, or complaints under regulations pertaining to the company. Incidents would be reported to the organization's incident response center.

Roles and Responsibilities

The clinic's IRT would oversee privacy incident management activities to confirm incidents are evaluated based on the level of risk. The IRT also verifies the response activities are relevant. The clinic's IRT management would provide direction to the IRT to carry out their specified roles and responsibilities. Doctor Dog would serve as the senior agency official for privacy and the IRT Chair. The clinic's IRT Coordinator, Doctor Cat, would validate that the performance of the IRT's duties are what is expected. Serving as the liaison between the operations and staff division, IT Manager, would be the IRT coordinator who would gather information after the initial notification. In addition, the coordinator becomes the information security subject

matter expert. In the case of loss, the insurance representative would be responsible for providing danger supervision and break down verification. An IT subject matter expert would also be involved in making proposals on the best way to mitigate an incident. A human resources representative would provide insight on dealing with laborers. Legal would be present to provide their expertise on any potential legal issues. Lastly, a public representative would advise on the most efficient way to provide information to the public and key customers.

Information Flow and Communication

Once an incident is declared, the DRT is mobilized. Network technical and administrative employees would assemble at designated locations immediately for alternate operations and communications. The emergency command centers are located in Maryland and District of Columbia areas and all points of contact would be the SME at that location.

Services Provided by IRT

The following services are provided by the clinic's IRT:

- Planning, individual of the key administrations to an answer arrangement is to perceive how to apply it simply once it is set up. The business has records for occurrences of various sorts and in addition phases of effect.
- Identification perceive whether and furthermore not an event has happened. Investigation of log records and additionally alerts will give the vital information for this progression.
- Control connects with restricting the degree and also size of an event.
- Elimination connects with expelling the reason of the event. This can be finished by re-establishing administrations and in addition game plans to the last perceived good state

furthermore by absolutely revamping it related on the design information that was before archived.

- Improvement is re-establishing an arrangement to its ordinary industry status. This assumes the nullification procedure was successful and that the administrations furthermore designs have been affirmed and affirmed as great.

Authority and Reporting

All activities will be reported to the IRT Chair. Everyone should be fully aware of the role in the event of a disaster or incident. All progression of this change technique might be recorded on an appropriate report layout. The report will contain highlights of the event, the names involved in the event, and an instance stamp. The IRT Chair will approve this portrayal to affirm it.

INFORMATION SECURITY PLAN

Overview

An Information Security Policy provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an Information Security Policy defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an Information Security Policy as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Information Security team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

Scope

This policy applies any established and defined business unity or entity within the Coastal Veterinary Clinic.

Ownership

This policy will be owned by the 2 Doctors that own the Coastal Veterinary Clinic, Dr. Cat and Dr. Dog. They will both be responsible for enforcing the Information Security Policy but Dr. Dog will take the primary responsibility and Dr. Cat will take the secondary responsibility. The Policy will be reviewed monthly by the Doctors and the IT Manager. Any modifications will be made after all three parties agree on the modifications.

Sanctions

Anyone found to have violated these policies may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. The first offense will require a one-hour training session with the manager. The second offense will require a one-day training session with the manager. The third offense may include termination.

Training

One method of ensuring that security policy is understood by general users is to provide training on the policies. This allows users to ask questions and receive specific guidance, and it allows the organization to emphasize key points. These general users also require training on the technical details of how to do their jobs securely, including good security practices, password management, specialized access controls, and violation reporting. A convenient time to conduct this type of training is during employee orientation. During this critical time, employees are educated on a wide variety of organizational policies and procedures and on the expectations the organization has for its employees. Because employees haven't yet established preconceived notions or methods of behavior, they are more likely to be receptive to this instruction. This is balanced against the fact that they are not yet familiar with the systems or their jobs; therefore, any particular issues that they might have questions about won't have arisen. Technical training for IT staff, security staff, and technically competent general users is more detailed than general user or managerial training, and it may therefore require the use of consultants or outside training organizations. Monthly training sessions of one hour will be required as well.

Sensitive Data Inventory

The sensitive data that the Coastal Veterinary Clinic owns is from the clients, dogs and cats as well as employee data. The financial data is also sensitive. The data is stored on the servers in IT closet. The clinic is fully digital and doesn't have paper data.

Incident Response

The 2 Doctors that own the Coastal Veterinary Clinic, Dr. Cat and Dr. Dog is responsible for handling information security incidents. They will use a call tree to notify the IT Manager, then the employees and the clients if needed.

Backups

The backup of data stored on individual workstations, including software and database data must receive a full backup on a daily basis. System and application data are to be backed up with at least one full backup using the generation principle. All weekly backup media must be stored in a fireproof safe. All full backup media must be stored in an off-site backup archive storage location. Each data backup process should have at least one primary backup administrator and one secondary. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.

The backup administrator should document the following items for each generated data backup:

- Name of backup media describing data contents
- Date of data backup
- Type of data backup (incremental, full)
- Backup administrator
- Storage location of backup copies

The restoration of data using data backups must be tested periodically to ensure that complete data restoration is possible to ensure whether:

- Data restoration is possible
- The data backup procedure is practicable
- Data backup procedures are documented properly
- The time required for data restoration meets the availability requirements

Clean Desk & Workstation Locking

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period. Computer workstations must be locked when workspace is unoccupied. On a Windows machine, you can do this quickly with Windows key + L. Mac users can use Control+Shift+Power, or if you have an older model use Control+Shift+Eject instead. Computer workstations must be shut completely down at the end of the workday. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk. Laptops must be either locked with a locking cable or locked away in a drawer

Acceptable Use: Computers

Keep business and pleasure separate: don’t connect personal devices to the business network. Charging your phone from the office computer sounds innocent enough but remember that

smartphones can also be infected with malware without showing any obvious signs. An infected device can transfer unwanted software like keyloggers to the computer, which allow an attacker to track every keystroke that is typed on the computer, providing unwanted access to any piece of software or confidential data on the computer.

Take it slow and first determine if hyperlinks in emails are safe to open. Phishing is an attempt to steal your personal details by using an e-mail that appears as if it comes from a familiar and trusted source: Such an e-mail might look innocent but often in the message the attacker will, for instance, urge you to log in to your bank account, thus gaining access to sensitive information like passwords, account numbers and personal details. Since reputable businesses and government entities will never ask you for username and password details, the best solution is to mark such messages as spam and immediately delete them.

Acceptable Use: Internet

Internet access is intended for business use, instruction, research and the facilitation of communication, collaboration, and other Coastal Veterinary Clinic related purposes. Users have no right to privacy while using the Coastal Veterinary Clinic Internet Systems. The clinic monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on Coastal Veterinary Clinic provided devices, such as files, e-mails, cookies, and Internet history.

The clinic reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent

with applicable law. The clinic will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the Coastal Veterinary Clinic's Internet Systems. Users may not engage in any of the activities prohibited by this policy when using or accessing the Coastal Veterinary Clinic's Internet Systems.

Causing harm to others, damage to their property or Department property, such as:

- Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, material posted on Coastal Veterinary Clinic's web pages, or professional social media sites;
- Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school or central division office;
- Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
- Sending, posting, or otherwise distributing chain letters or engaging in spamming;
- Damaging computer equipment, files, data or the Department's Internet System in any way, including spreading computer viruses, vandalizing data, software or equipment, damaging or disabling others' electronic property, or engaging in conduct that could

interfere or cause a danger of disruption to the Department's educational or business environment;

- Using the Coastal Veterinary Clinic's Internet System in a manner that interferes with the education of the user or others or the job duties of the user or others;
- Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws. Any music, photographs and/or video should only be downloaded for clinic, and not personal purposes. If a work specifies how that work may be used, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright or trademark owner; or
- Engaging in plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Malicious tampering, phishing or hacking activities;
- Intentionally seeking information about passwords belonging to other users;
- Modifying passwords belonging to other users;
- Attempting to log in through another person's account;
- Using the password or identifier of an account that does not belong to the user; or
- Engaging in uses that jeopardize access into others' accounts or other computer networks.

Acceptable Use: Laptops

Often at home or in at the vet practice, you'll be sharing a laptop or workstation with multiple users. Always using your own login account and logging off once you're finished is an important start to keeping the device cyber safe. Also be sure to log out of any websites or programs you were using, and never allow your browser to save passwords or login information. This will help prevent others from purposely or accidentally logging into your accounts and accessing your information. All laptops and walking devices should be used in conjunction with a token device to prevent any unauthorized use. Any employees working from home should only access the network through a secure VPN, and again, use tokens to verify their identity.

Acceptable Use: Mobile Devices

The use of personal devices is limited to employees and may be limited based on compatibility of technology. To ensure the security of Coastal Veterinary Clinic's information, authorized employees are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. Coastal Veterinary Clinic's IT department must install this software prior to using the personal device for work purposes. Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

Acceptable Use: Remote Access

Remote access allows a user, or a group of users the ability to interface with a private network through the internet. Limited access to the server remotely is the best possible choice is limited the possibility of compromise among the connections of the server. I think the remote access policy would dictate what connections would be allowed or rejected when it comes to connecting with the network itself, be it through dial-up, or a virtual private network. The group policy should validate a number of factors before authorizing the connections much like a group message, the of connection, the time of day or whether an unauthorized access is allowed. Incorporating this access control policy and all of its parts will help keep the system secure and safe while ensuring that everyone that has access to the network is authenticated ad protected in the future.

Acceptable Use: Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks

such as CD and DVD disks; floppy disks and software disks not provided by Coastal Veterinary Clinic.

Acceptable Use: Social Media

Social media can take many different forms, including internet forums, blogs & microblogs, online profiles, wikis, podcasts, pictures and video, email, instant messaging, music-sharing, and voice over IP, to name just a few. Examples of social media applications are LinkedIn, Facebook, Myspace, Wikipedia, YouTube, Twitter, Yelp, Flickr, Second Life, Yahoo groups, WordPress, ZoomInfo – the list is endless. When you are participating in social networking, you are representing both yourselves personally and Coastal Veterinary Clinic. It is not our intention to restrict your ability to have an online presence and to mandate what you can and cannot say.

- Do not post any financial, confidential, sensitive or proprietary information about Coastal Veterinary Clinic or any of our clients and candidates.
- Speak respectfully about our current, former and potential customers, partners, employees and competitors.
- Use privacy settings when appropriate. Remember, the internet is immediate, and nothing posted is ever truly private nor does it expire.
- If you see unfavorable opinions, negative comments or criticism about yourself or Coastal Veterinary Clinic, do not try to have the post removed or send a written reply that will escalate the situation.

Vulnerability and Patch Management

Patch all critical and high vulnerabilities within 15 and 30 days, respectively, on internet-accessible systems. Be sure to scan for configuration vulnerabilities in addition to software vulnerabilities. Enable automatic updates whenever possible. Replace unsupported operating systems, applications, and hardware.

Network Security

Configure the network perimeter to deny all incoming traffic that is not expressly permitted. Properly secure all remote access methods, including modems and VPNs. An unsecured modem can provide easily attainable unauthorized access to internal systems and networks. War dialing is the most efficient technique for identifying improperly secured modems. When securing remote access, carefully consider the trustworthiness of the clients; if they are outside the organization's control, they should be given as little access to resources as possible, and their actions should be closely monitored. Put all publicly accessible services on secured demilitarized zone (DMZ) network segments. The network perimeter can then be configured so that external hosts can establish connections only to hosts on the DMZ, not internal network segments. Use private IP addresses for all hosts on internal networks. This will restrict the ability of attackers to establish direct connections to internal hosts. Perform regular vulnerability assessments to identify serious risks and mitigate the risks to an acceptable level. Disable all unneeded services on hosts. Separate critical services so they run on different hosts. If an attacker then compromises a host, immediate access should be gained only to a single service. Run services with the least privileges possible to reduce the immediate impact of

successful exploits. Use host-based/personal firewall software to limit individual hosts' exposure to attacks. Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office. Regularly verify the permission settings for critical resources, including password files, sensitive databases, and public Web pages. This process can be easily automated to report changes in permissions on a regular basis. Create a password policy that requires the use of complex, difficult-to-guess passwords, forbids password sharing, and directs users to use different passwords on different systems, especially external hosts and applications. Require sufficiently strong authentication, particularly for accessing critical resources. Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software. For example, passwords should be strongly encrypted using a FIPS 140-validated algorithm when they are transmitted or stored. Establish procedures for provisioning and deprovisioning user accounts. These should include an approval process for new account requests and a process for periodically disabling or deleting accounts that are no longer needed.

Wi-Fi Security

Coastal Veterinary Clinic shall manage and control its wireless networks in order to protect Coastal Veterinary Clinic data and other information assets that access, traverse, or reside within the Coastal Veterinary Clinic network. A current wireless network diagram shall exist and shall be updated whenever there are network changes and no less than every 6 months. The wireless network diagram shall be made immediately and continuously available for Coastal Veterinary Clinic official operational, planning, and coordination purposes. Vendor defaults for

wireless access points shall be changed prior to authorizing the implementation of the access point. At a minimum, this includes changing the manufacturer's default settings for encryption keys, SSIDs, known and trusted wireless devices, and passwords. Wireless access points shall be configured with strong encryption (WPA2 at a minimum). Wireless access points shall be placed in secure locations unless otherwise approved by the Chief Information Security Officer (CISO). File sharing shall be disabled on wireless-enabled devices. All wireless network devices shall be identified and authenticated prior to establishing a connection. Only wireless access points expressly authorized by the CISO shall be permitted to establish a connection. Firewalls shall be configured to deny by default (deny all, permit by exception) or control any traffic from a wireless environment into the confidential data (e.g., PHI, SSN, PII) environment. Wireless networks shall be monitored and audited for policy compliance. Wireless network use shall be subject to all applicable HSX policies. The guest wireless network shall not connect to the Coastal Veterinary Clinic wireless network. Coastal Veterinary Clinic shall reserve the right to prohibit or deny connections to its wireless networks at any time for any reason.

Email Security

Cyber security awareness training is vital for every employee. When one of your employees receives a phishing email with some type of an attachment. The employee can choose to flag the email as junk or spam and send an email to the IT manager to let them know about what just occurred.

Antivirus programs come equipped with many features — and mail filters and scanning capabilities for files and websites may be among them. If so, put these capabilities to work for

your advantage. These can help you identify some forms of malware and other threats to help prevent your devices or network from becoming infected. If you can, set the antivirus program to work with your mail proxy/relayer to scan emails to filter out potentially malicious emails to keep them from being delivered to your (or your employees') inboxes.

Create email blacklists and whitelists. Blacklists can be maintained by domain, email address, and IP address/range. The whitelist is a list of email addresses that are permitted through your filters and server. This list can be maintained through those same three components (domain, email address, and IP address/range).

Require that employees use strong passwords. Includes a combination of upper and lowercase letters, numbers, and symbols. Avoids using words that can be found in the dictionary. Does not include the names of your pets, family members, favorite teams, or other information that can be found easily on your social media profiles. To make your password more guess-resistant if you want to use words that are semi-easy to remember, intersperse numbers or symbols in place of letters throughout them. For example, instead of using *kittycat* or *ilovecatssomuch* as your password, use something like *K17tyC@t!* or *I<3C@tSs0Muc#*.

Use the S/MIME protocol for data encryption and email signing. Enter S/MIME, or the "secure/multipurpose internet mail extension (S/MIME) protocol" an advanced email security best practice. This term refers to an email signing protocol that increases email security by creating a timestamped digital signature to confirms the sender's identity to the recipient;

encrypting and decrypting the contents of emails to provide at-rest and in-transit data protection; and facilitating the secure sharing of documents across networks.

Website Security

Secure domain ecosystems.

- Review registrar and Domain Name System (DNS) records for all domains.
- Change all default password that were provided from your domain registrar and DNS.
    - Default credentials are not secure—they are usually readily available on the internet. Changing default usernames and passwords will prevent an attack that leverages default credentials
- Enforce multi-factor authentication (MFA).
- Monitor certificate transparency logs.

Secure data in transit.

- Disable Hypertext Transfer Protocol (HTTP); enforce Hypertext Transfer Protocol Secure (HTTPS) and HTTP Strict Transport Security (HSTS).
    - Website visitors expect their privacy to be protected. To ensure communications between the website and user are encrypted, always enforce the use of HTTPS, and enforce the use of HSTS where possible
- Disable weak cyphers (SSLv2, SSlv3, 3DES, RC4).

Secure web applications.

- Identify and remediate the top 10 most critical web application security risks; then move on to other less critical vulnerabilities
- Enable logging and regularly audit website logs to detect security events or improper access.
    - Send the logs to a centralized log server.
- Implement MFA for user logins to web applications and the underlying website infrastructure.

Secure web servers.

- Use security checklists.
    - Audit and harden configurations based on security checklists specific to each application Apache and MySQL on the system.
- Use application allow listing and disable modules or features that provide capabilities that are not necessary for business needs.
- Implement network segmentation and segregation.
    - Network segmentation and segregation makes it more difficult for attackers to move laterally within connected networks. For example, placing the web server in a properly configured demilitarized zone (DMZ) limits the type of network traffic permitted between systems in the DMZ and systems in the internal corporate network.

- Increase resource availability. Configure website caching to optimize resource availability. Optimizing a website's resource availability increases the chance that it will withstand unexpectedly high amounts of traffic during DoS attacks.
- Implement cross-site scripting (XSS) and cross-site request forgery (XSRF) protections. Protect website systems, as well as website visitors, by implementing XSS and XSRF protections.
- Implement these additional security measures:
    - Running static and dynamic security scans against the website code and system,
    - Deploying web application firewalls,
    - Leveraging content delivery networks to protect against malicious web traffic, and
    - Providing load balancing and resilience against high amounts of traffic.

Endpoint Security

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats. McAfee offers endpoint security that includes an Endpoint Detection and Response (EDR) component. EDR capabilities allow for the detection of more advanced threats, such as polymorphic attacks, fileless malware, and zero-day attacks. By employing continuous monitoring, the EDR solution is able to offer better visibility and a variety of response options.

Server Security

Primary methods that organizations use to protect against loss of availability are fault tolerant systems, redundancies, and backups. Fault tolerance means that a system can develop a fault but tolerate it and continue to operate. This is often accomplished with redundant systems such as redundant drives or redundant servers. Backups ensure that that important data is backed up and can be restored if the original data becomes corrupt. Fault tolerance and redundancies can be implemented at multiple levels. For example, RAID-1 is a mirror of two drives; if one drive fails, the other drive still holds all the data. RAID-5 (striping with parity) uses three or more drives and uses parity to recreate the data if any drive fails. RAID-10 combines the features of a RAID-1 with the features of a RAID-0 array. You can add redundancies for servers by configuring them in a failover cluster. Failover clusters include two or more nodes (servers within the cluster) and if any node fails, other nodes can take over. This happens automatically with very little impact on end users.

Access Control: Onboarding

User enrollment: Upon the first login of the user, he/she will be able to self-enroll into the system via an activation link given to them by the system administrator. This link will set the user through a number of steps that enroll them into the system as an employee. Upon the last step, the user agrees to a policy that is given to him. The employee's rights will be adjusted in group policy under remote access setting. Due to time sensitivity and possibility of a threat, the links for enrollment will be set to expire 24 hours after it is given. If the user does not enroll in that time, they will have to get a new link for enrollment from the tech support or help desk.

Identification will be confirmed through a two-step process. How the information is gathered up to the employer and how the steps are given is also up to the employer. Step 1: Specific questioned asked during the first initial step of hiring would be used to compile questions that help identify the user. Step 2: Information gathered from public records will be used to assist in determining the user's identity. Information such as previous places of residence, previous jobs, or last school attended. Authentication is gained by the answering correctly questions asked during the identification process. All questions must be answered correctly, and promptly. If once an answer is wrong authentication fails, and privilege is denied as well as access. When authentication is achieved. The user will be given specifics to what they are allowed and not allowed to do. In the end, and once identification of the user is complete the user is taken through a PAP, or password authentication protocol to create their password that they will be using at a later time to log into the server from then end on.

Access Control: Physical

Network or server equipment: A secure room with restricted access is needed for storing all network and server equipment. Ventilation and temperature control are also required to protect the equipment from overheating. This should be a room that is protected from environmental damages such as fire and rain. Locking server racks should be used as a secondary security measure.

Access Control: Job Changes

When someone changes their role, their levels of access will be changed as appropriate to their new role. A privileged access management system will be used to make the changes and keep the records of past roles and privileges.

Access Control: Terminations

When employment is terminated by either party, the clinic or the employee, all access will be turned off immediately.

Passwords

Upon the first login of the user, he/she will be able to self-enroll into the system via an activation link given to them by the system administrator. This link will set the user through a number of steps that enroll them into the system as an employee. Upon the last step, the user agrees to a policy that is given to him. The employee's rights will be adjusted in group policy under remote access setting. Due to time sensitivity and possibility of a threat, the links for enrollment will be set to expire 24 hours after it is given. If the user does not enroll in that time, they will have to get a new link for enrollment from the tech support or help desk.

Encryption Key Management

Encryption converts plain text data into ciphered data. Ciphered data can't be read (at least not easily) if received or intercepted by unauthorized individuals. It's estimated that it'll take hundreds of years for an attacker to crack many of the strong encryption methods in use today. In contrast, weak encryption methods (like WEP used with older wireless networks) can be cracked in seconds with the right software. Many types of encryption algorithms are popular today. The Advanced Encryption Standard (AES) is a fast, efficient algorithm that is commonly used to encrypt data at rest. Trusted Platform Modules (TPMs) can encrypt entire hard drives which is especially useful for portable computers. S/MIME is used to encrypt (and digitally sign) email. Many other protocols such as SSL, TLS, IPsec, and others encrypt data sent over the wire either over the Internet or on internal networks. One of the common ways of ensuring integrity

is with hashing. In short, a hash is a number and a hashing algorithm can calculate a hash for a file or string of data. As long as the data has not changed (and the same hashing algorithm is used), the hash will always be the same. The two primary hashing algorithms used today are Message Digest 5 (MD5) and Secure Hashing Algorithm 1 (SHA-1) As an example, if you calculate the hash of the phrase “CyberCorps” with the MD5 hashing algorithm it will always be E7F8B292F4F5C2F98E5DF1435EB73D1B. However, if the phrase is slightly modified to “CyberCarps” (the “o” is change to an “a”) the hash is 2F088A01343CFD65B7BC4EB050503CB7. By comparing the two hashes and seeing that they are different, you know that the original data created by each of the two hashes are different.

Database Security

Database security encompasses multiple controls, including system hardening, access, DBMS configuration, and security monitoring. These different security controls help to manage the circumventing of security protocols. It is vital that all systems are patched consistently, hardened using known security configuration standards, and monitored for access, including insider threats. It is critical that the DBMS be properly configured and hardened to take advantage of security features and limit privileged access that may cause a misconfiguration of expected security settings. Monitoring the DBMS configuration and ensuring proper change control processes helps ensure that the configuration stays consistent. Database security measures include authentication, the process of verifying if a user’s credentials match those stored in your database, and permitting only authenticated users access to your data, networks, and database platform. A primary outcome of database security is the effective limitation of access to your data. Access controls authenticate legitimate users and applications, limiting

what they can access in your database. Access includes designing and granting appropriate user attributes and roles and limiting administrative privileges. Monitoring (or auditing) actions as part of a database security protocol delivers centralized oversight of your database. Auditing helps to detect, deter, and reduce the overall impact of unauthorized access to your DBMS. Database security can include the secure management of encryption keys, protection of the encryption system, management of a secure, off-site encryption backup, and access restriction protocols. Database and application security framework measures can help protect against commonly known attacker exploits that can circumvent access controls, including SQL injection.

Physical and Facility Security

Having perimeter security, such as fencing would be the first layer of security to implement. The following step would be to include a recognized identification system Items such as badges, keys, or smart cards are used in this layer to access the facility. The implementing of a surveillance system at the gates or each of the entrances is another layer of protection. All physical entry points not classified as publicly accessible have been fitted with a keypad and id badge scanner combination. These points allow personnel employee entry into work areas while keeping out the customers and the public. Motion detection systems and an alarm system would provide a layer of protection during off hours. Isolated delivery and loading areas where deliveries are unloaded or loaded is to remain locked unless currently in use. Large doors are only opened from the inside and unlocked when a key card is used, and the mag lock is disengaged. Inside the building should have security cameras in each area covering all angles of each area.

Revision History

Revision No.	Date	Description of Changes	Authorization

Plan Distribution & Access

The Plan will be distributed to members of the Business Continuity Team and key employees. A master copy of the document should be maintained by the IT Manager in concert with Doctor Dog. Provide print copies of this plan within the room designated as the emergency operations center (EOC). Multiple copies should be stored within the EOC to ensure that team members can quickly review roles, responsibilities, tasks, and reference information when the team is activated. An electronic copy of this plan should be stored on a secure and accessible website that would allow team member access if company servers are down. Electronic copies should also be stored on a secure USB flash drive for printing on demand.