WELLNESS TECHNOLOGY
We Bring Technology to Life

Wellness Technology

Incident Response Plan

___Working Draft ___Approved ___Adopted

Document Creator: Clifton Gibbons

Last Review Date: ____________________________

Version	Modified Date	Approved Date	Author	Comments
1.0.0	**March 2021**		**Wellness Technology**	**Document Origination**

Confidential Information: This document may contain information that in privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior authorization by Tier 1/2 Administration.

Table of Contents

Introduction

The **Wellness Technology** ***Incident Response Plan*** has been developed to provide a direction and focus to addressing unique physical and information security incidents that may adversely affect the day-to-day functions of **Wellness Technology's** physical structure and information systems and security infrastructure. The ***Incident Response Plan***, henceforth known as the IR Plan, will apply to all persons and entities charged by Wellness Technology's Incident Response Organizers (IRO) with responses to both structural and information security related incidents for the organization. IRO-1 will manage structural related matters and the IRO-2 will manage Information Systems related matters.

Purpose

The purpose of the IR Plan is to allow Wellness Technology to respond quickly and appropriately to adverse structural and information systems/security related incidents.

Event Definition

Any observable instance of an event in a network, system, environment, process, workflow, communication, personnel, early warning system(s) or physical structure(s). These events may or may not be negative in nature.

Adverse Events Definition

Event with negative consequences. This plan only applies to adverse events that are either man made or natural disaster related incidents.

Incident Definition

Physical Structures

Acknowledgement of man made or "act of God" destruction to physical structures that jeopardizes or impedes the facilities daily service functions.

Information Systems

A violation of, imminent threat to or inadvertent consequence of established security policies, acceptable use policies, standard security practices and/or failure of intermediary services that jeopardize the confidentiality, integrity and/or availability of information resources or operations.

Contact Information

Updated March 1, 2021

Name	Title	Role	Phone Number	**Escalation Tier
Burt Jennings	VP of Operations	IRO-1	334-272-1111	1
Richard Sellers	Information Security Mgr.	IRO-2	334-272-1212	1
William Riddle	CIO	CIO	334-272-3714	2
Jennifer Idle	Communications Manager	*IRT – Public Relations	334-272-3918	3
Jaci Gutierrez	Risk Manager	*IRT – Risk Mgmt.	334-272-1244	3
Ben Yanko	President	*IRT – President	334-399-1818	3
Law Enforcement	Police	Law Enforcement	911	3

*IRT: The Incident Response Team

**Escalation level determines order in which notification should occur

1. Notify first, required on all incidents.
2. Required on all moderate or high-severity incidents
3. Involve as needed

Roles and Responsibilities

Incident Response Team (IRT)

- Consist of senior management, legal experts, risk management and other department managers that may be consulted or notified during an incident.
- Advise on incident response activities relevant to their area(s) of expertise.
- Maintain a general understanding of the IR Plan and Policies of the organization.
- Ensure that incident response activities are in accordance with legal, contractual, and regulatory requirements.
- Participate in organized testing of the IR Plan and Procedures

Each will be responsible in his/her own way for internal and external communications pertaining to incidents of physical and/or InfoSec matters.

Chief Information Officer (CIO)

- Seeks approval from Executive Management for the administration of the Incident Response Program.
- Coordinates response activities with auxiliary departments and external resources as needed to minimize damages to physical and IS infrastructure(s).
- Ensure service level agreements with service provides clearly define expectations of the organization and the service provider in relation to incident response.
- Ensure polices related to the Incident Response Plan accurately represent the goals of the organization.
- Ensures the IRT are given necessary authority to initiate repair services, seize assets and/or stop services quickly to mitigate further damages or contain moderate or critical-severity events.
- Approve close of moderate or critical-severity events
- Ensure lessons learned are captured and applied/weighed in respect to the risk for Severity 1 incidents.
- Create and disseminate after action report on all incidents and amend to annual company Health Report Card (HRC). The HRC submission period ends every calendar year on the 20th of December.

Incident Response Organizer – 1

The Incident Response Organizer – 1 oversees and prioritizes actions during the discovery, analysis and completion of repairs to the organization's physical infrastructure. They are also responsible for conveying any and all special requirements, physical upgrades and new installation of physical grounds equipment(s). Additionally, they will be responsible for establishing contracts/SLA's, coordinating service events, updating senior staff and supplying project completion reports for all incidents with their purview.

Incident Response Organizer – 2

The Incident Response Organizer – 2 oversees and prioritizes actions during the loss of critical communication services, detection, analysis and containment of any cyber event. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the CIO. Additionally, they are responsible for understanding the SLA's in place with third parties, and the role third parties may play in specific response scenarios.

Incident Response Framework

Wellness Technology recognizes that, despite best reasonable and competent efforts to protect both physical and information system infrastructures, the possibility of natural disaster, man made interference, breaches or other loss of building and/or information services is possible. The organization must make reasonable efforts to act competently to respond to these potential incidents in a way that reduces the damage/loss and mitigate potential harm to customers, partners and/or the organization itself.

Developing a well-defined incident response framework is critical to an effective incident response plan. Wellness Technology's incident response framework is comprised of six (6) phases that ensure a consistent and systematic approach.

Phase 1 - Preparation

It is essential to establish your Incident Response Team, define appropriate lines of communication, articulate the services necessary to facility a response and procure all necessary tools.

Phase 2 – Identification and Assessment

Identifying and event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, all evidence – physical and digital – will be preserved while any forensic analysis can be conducted consistent with all legislative and/or legal requirements.

Phase 3 – Stop Gap and Containment

Stop Gap and Containment is necessary to minimize and isolate damage(s) observed. Steps must be taken to ensure that the scope of the incident does not progress further. A Root Cause analysis is required prior to moving beyond the Stop Gap and Containment phase and may require expertise from outside parties.

Phase 4 – Redressing

Redressing requires the initiation of repair and/or removal of all components and elements of the incident. Further validation must be performed to ensure that the incident is both stable and free from defect. In Information System Infrastructure, validation will be used to help ensure the incident does not reoccur.

Phase 5 – Recovery

Recovery involves the steps required to restore full functionality of services to a healthy working state allowing business operations to be returned.

Phase 6 – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the infrastructure(s) that were impacted by the incident and other potentially vulnerable infrastructure elements. Lessons learned from the incident are communicated to executive management in the Health Report Card and action plans are developed to improve future incident response practices to reduce the risk of future events.

Wellness Technology Incident Response Model

The Wellness Technology IR Plan is based off of the SANS PICERL Incident Response Model; however, alterations were made to allow a cohesive fit for the organization's model.

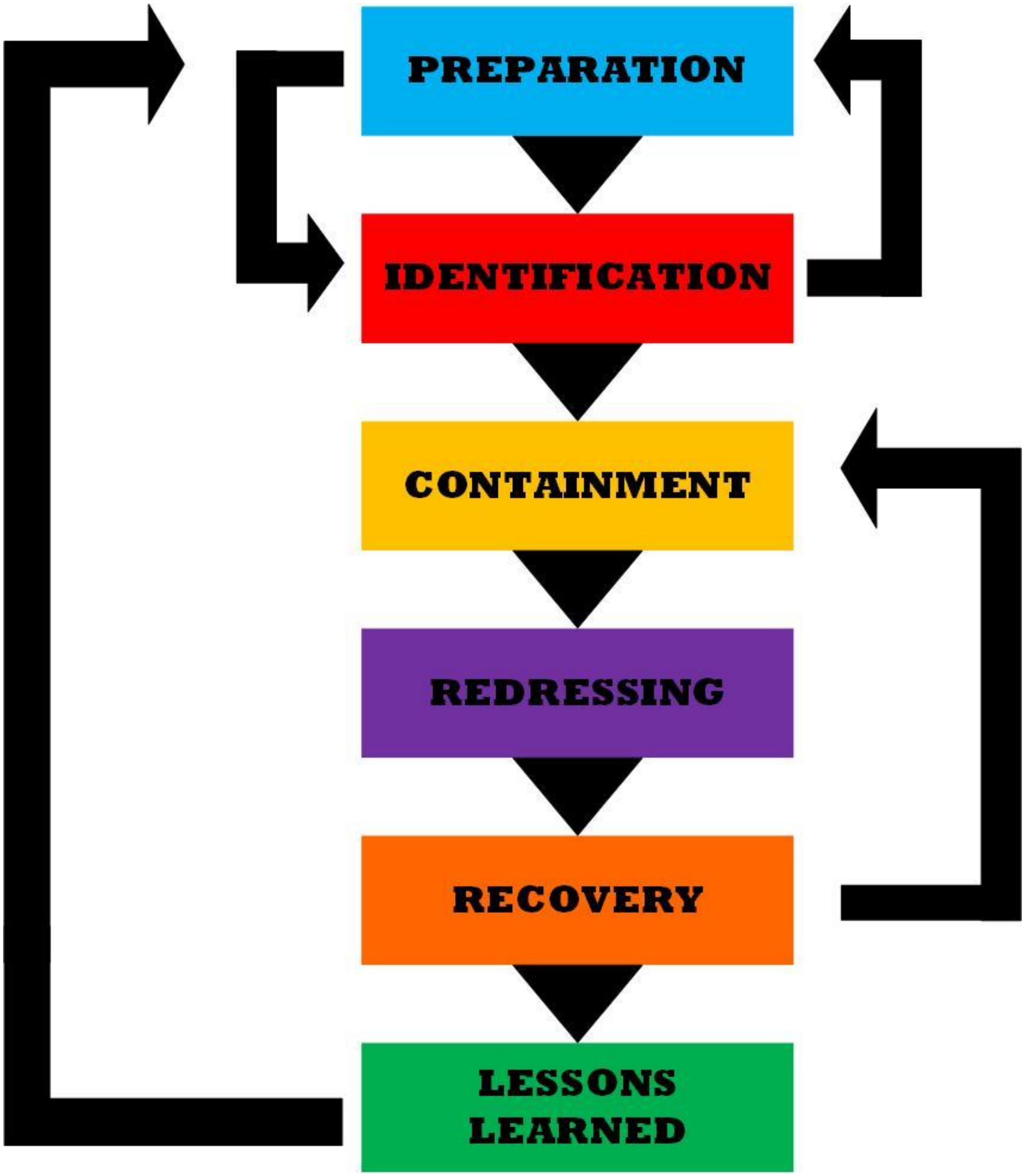

Figure 1: Wellness Technology Incident Response Model

Based off of the SANS PICERL Incident Response Model

Power Failure

Although power failure is not a typical element faced by organizations, it is mission critical to ensure service functionality. The Power Failure Incident Response will detail the 6-phase strategy to restoring services. As each instance of power failure is unique, these steps are in broad terms and may evolve during the course of the incident.

Phase 1

Inspection and Testing

- Generators will be tested Semi-Annually
- Worn equipment will be replaced upon discovery
- Power Outage simulation will be performed once per year

Staff Training

- Virtual training session: What to do When the Lights Go Out

Phase 2

- Identify source of outage
- Unless serious hazard involved, notify on Escalation Level: 1 only
- Refer to SLA’s/Contracts and address with vendors.
- Obtain outage approximation
    - If generators will hold during outage approximation, maintain staff onsite
    - If generators will exhaust before power restoration, submit request for staff dismissal.

Phase 3

- Ensure that generator power is assigned to highest priority devices/electronics
    - Non-essential items should be turned off and unplugged for power conservation

Phase 4

- Maintain constant communication with vendors to ensure outage approximations remain consistent.
    - In the event power loss estimations evolve and are prolonged, evaluate generator usage and inform of potential service interruptions.

  - Return to discussion of staff dismissal

Phase 5

- Power is restored
  - Ensure generator is reserving stores
  - Ensure non-essential devices are plugged in and restored to service
  - Monitor for possible rolling interruptions due to loss
- Ensure staff are restored to full service

Phase 6

- Document steps taken to ensure service
- Document service of generators
  - Did they function to specifications?
  - Did they use too much power outside of specifications?
- Notate outage time and review annually for potential anomalies

Internet Service Provider (ISP) Failure

Internet services are critical in the mission of Wellness Technology. As our offices gear towards providing both online transaction processing and live remote services. The ISP Failure section discusses processes to addressing the loss of internet services using the 6-phase process. As this incident is narrowly defined in occurrence, resolution steps will relatively straight forward.

Phase 1

Service Provider Evaluation

- Research provider reliability
- Discuss mitigation/restoration measures within the providers framework
- Create action plan with service provider on alternate connectivity methods

Equipment Maintenance

- Evaluate network equipment Semi-Annually
- Determine new technology and evaluate effectiveness
- Replace worn equipment when viable and remove dust particulates when possible.

Phase 2

The IRO-2 will confirm that there is a network outage that is affecting all users. The manner of determining this will be via communication efforts between various department managers, and the IT Department’s evaluation of network services.

Phase 3

In order to contain damage based on loss, management will be notified of the network loss, provided and ETA (if available) and to implement manual services where available. For remote services, customers will be informed of technical difficulties using pre-defined “talk tracs” developed for each department. (See Manager for talk trac information)

Phase 4

- Report unusual/sporadic connectivity issues
    - Speed/Data Packet loss
    - Random connection loss
- When connection is lost
    - Ensure issue is not isolated
        - If isolated, evaluate network switch and other connected network components.
    - Reboot internet services equipment
    - Run network viewer (Wireshark) to ensure valid network traffic
    - Evaluate equipment for blinking interruption lights
        - Typically, red blinking lights
    - Ensure power to equipment
- If troubleshooting steps fail, contact service providers and enforce SLA’s as needed.
- Implement secondary network measures as needed
    - Secondary measures include the use of MiFi products and Dial-up services.

Phase 5

Once services are restored, management will confirm that their teams are functional and have full network access. Once confirmed, they will report their status to the IRO-2. Instances of down/degraded services will be evaluated by Wellness Technology’s IT Department for anomolies in network traffic. Once fixed, both IT and the department manager will submit notification of service restoration to the IRO-2

Phase 6

The IRO-2 will conduct a network evaluation in conjunction with the IT Department. Their assessment will be presented to the CIO for evaluation. The CIO will take the findings of the IRO-2 and IT Department and create a detailed report for review in the Health Report Card for Wellness Technology. The CIO, as needed, will share his/her comments on additional products based on the findings of the IRO-2 and IT Department evaluation and submit in their report.

Fire

Fire damage is a destructive element to every business; however, ensuring you have a well-defined plan of action will help navigate the circumstances and minimize critical loss of service as well as save the lives of both staff and customers. Wellness Technologies has implemented the following 6-step fire response plan.

Phase 1

Inspection, Testing and Equipment

- A quarterly evaluation of all fire equipment will be conducted. Results will be provided to the IRO-1 for review
- Removal and Replacement of expired equipment will be performed upon discovery
- Replaced items will be submitted to the IRO-1 for documentation

Training

- Employees must complete an annual exam on Fire Safety and Emergency Evacuation procedures.

Phase 2

Fire Alarm

Well Technology’s fire alert services are professionally installed and managed by staff. The fire alarm system is a 120-decibel alarm with strobing lights. Users will hear or see the alarm with tripped and follow emergency evacuation procedures. The IRO-1 manages until all clear. Reports “All Clear” to management.

Fire Observation

In the event a fire has been observed/discovered, the employee, or member of management, must activate the fire alarm system at their nearest location. Employees are, at this time, required to leave the building and follow their emergency evacuation procedures. IRO-1 and IRO-2 manage simultaneously to migrate services to the Warm Site and begin repairs to home office

Phase 3

- In the event that a fire alarm is triggered, management and team leaders will direct staff to the nearest available exit. Should the exit be blocked, alternate routes will be explained by the team leader/manager.
- Employees are to leave all equipment and exit the building, and they will meet in the assigned "Safe Harbor" location
- Managers/Team Leaders will perform a head count to ensure all members have evacuated safely.
    - If a member is not found, the manager/team leader is to report it to a member of the IRT immediately.
- Simultaneously, A member of the IRT will contact first responders with an alert of the fire alarm.
- Team Leaders and Managers will close all doors in their local area
- Employees, Team Leaders and Management should maintain heightened awareness of both sounds and odors and report them immediately.
- No employee will be allowed to re-enter the facility until an "All Clear" notification has been delivered from first responders.

Phase 4

Fire Alarm

- Upon successful evaluation of the facility, employees may re-enter with an "All Clear" notification from first responders.

Fire Observation

- Employees will not be permitted to re-enter the building until an "All Clear" has been given by first responders.

- Upon an "All Clear", employees may gather their belongings and return to the "Safe Harbor" location and await instructions from management.
  - If little damage has occurred, employees may resume regular duties.
  - If the damage is severe or may impede on safe working conditions, employees will be dismissed for the remainder of the day.

Phase 5

Fire Alarm

- Upon a successful evaluation of the facility, employees may re-enter with an "All Clear" notification from first responders.

Fire Observation

- If little damage has occurred, employees may resume regular duties
- If the damage is severe or may impede on safe working conditions, employees will be dismissed and provided instructions to the Disaster Recovery Warm Site
  - Each Manager will instruct his/her staff on directions to and contact information.
- The IT Department will begin opening proceedings on the Warm Site and notify the IRO-2 of their progress. The IRO-2 will update the CIO and Senior Management on the site progress
- Upon completion of the Warm Site, the IRO-2 will inform the CIO of completion. The CIO, will at this time, notify managers and senior management of the site status.

Original Facility Transfer

- Once repairs have been complete and an all clear provided by the IRO-1, the IRO-2 will dispatch the IT Department to begin network restoration.
- Upon completion of network restoration, the IT Department will notify the IRO-2 and the CIO.

Phase 6

- Cause of the fire is evaluated and documented.
- Implementation of corrective action performed to ensure no future reoccurrences
- Time constraints noted for transition to the Warm Site and/or Re-Entry
- Full Report created and documented or Health Report Card entry.

Water Damage

As we live in an area that is prone to various types of water concerns, our greatest concern is that of broken water pipes. Water damage can destroy technology as well as general every equipment and furnishings. So, mitigating water damage is crucial to Wellness Technology. The following 6-phase plan will stand a means to mitigate such damage.

Phase 1

Inspection and Winterizing

- An annual review of water and sewage services will be performed by contracted providers.
- Winterization of pipes will be conducted as needed
- Leaks and broken components will be addressed as discovered

Phase 2

As employees find potential water leakage or broken plumbing, these should be reported immediate to the IRO-1. The IRO-1 will assess the damages and determine the best course of action. Upon completing his/her assessment, they will report their findings to the IRT on a Escalation Level 1.

Phase 3

In order to contain potential damage, the IRO-1 may…

- order to turn off water supplies to this affected location
- erect a “Closed” or “Out of Order” notification
- place a covering over the affected item
- send out mail notifications of the affected area being closed

Phase 4

In order to redress the leak, the IRO-1 will contact contracted plumbing services to make the necessary repairs. In addition to making repairs, the IRO-1 may require a secondary inspection for additional leaks through the affected area.

Phase 5

Upon completion of services

- water is restored to the affected area
- all “Closed” or “Out of Order” signs will be removed
- all coverings will be removed.
- Notify users that services have been restored.

Phase 6

- Document specifics of the service issue
- Notate what items used to repair and repair costs
- Notate additional findings as needed
- Evaluate effectiveness of communication methods
- Create report for the Health Report Card (HRC)

Communications Failure

Equally important to Wellness Technology, with respect to internet, is the use of telecommunications services. Wellness Technology utilized the Voice over IP services (VoIP) to conduct daily service transactions and service calls. Loss of such an important service can be devastating to the organization. To mitigate this loss, the following 6-steps are in use.

Phase 1

Inspection

The VoIP services are evaluated one yearly as their services are a provision of Cisco services and utilized via the organizations Internet Service Provider. The analytics of the evaluation are conducted by Cisco and supplied to Wellness Technology.

Software

Software updates are performed every 1st Monday of the month. These software updates are evaluated and tested to ensure little to no interruption in service. Testing is performed by Wellness Technology’s IT Department.

Phase 2

Upon notification that telecommunication services are not available, the IT Department will notify the IRO-2 and the CIO. The interruption will follow an Escalation Level 2 scenario.

Phase 3

In order to contain damage to the company brand, the IT Department will update the Phone services Voice Recorded Updates (VRU) using a company issued cellular device. A "talk trac" has been created to update the recorded message along with alternate numbers for immediate service.

Phase 4

As a back to service, the IT Department will issue telephone systems that utilize Plain Old Telephone Service (POTS) that was installed for back up services. Telephone services will be routed in via the POTS service.

Phase 5

As services are being restored, the following will be conducted

- Line quality testing
- Packet quality evaluation
- Reset of phone network services
- Upload of phone service clone file
- Updates to the VRU

Phase 6

At this point in time, the IRO-2 should notate specifics of the incident such as

- Duration of outage
- Branding concerns as presented
- Issues restored service
  - What was done to restore service
- Create report for Health Report Card (HRC)

Software Security Failure

Wellness Technology's ***HealthTech*** services application is a what drives Wellness Technology's growth in the industry. As a technology leader, security is valued highly; however, no device or application is impervious to attack. Should the application face vulnerability from a virus or other malicious code, the following 6-steps are in place to mitigate such attacks and help maintain security.

Phase 1

Testing

Wellness Technology has enlisted annual penetration testing from ethical penetration testers (i.e. White Hat Hackers) to help harden security services surrounding the organization's ***HealthTech*** application and additional services.

Security Appliances

Implementation of firewall technology, DMZ's and Intrusion Prevention devices play a pivotal role in stopping potential attacks. As with other security elements, these devices are continuous updated and monitored for intrusion opportunities.

Incident Handling Team

In addition to an Incident Response Team, the IT Department will have an Incident Handling Team. This team will monitor and report on potential intrusions as well as injection of malicious code. They will…

- Ensure appropriate parties are aware of incident reporting processes
- Document and share cyber insurance details with appropriate parties
- Validate Logging, Alerting, and Monitoring policy compliance
- Review Penetration Test reports and validate remediations to findings
- Review Vulnerability Management reports and validate remediation efforts

Phase 2

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all of the following:

- Email or phone notification from an intrusion detection tool.
- Suspicious entries in system or network accounting, or logs
- Discrepancies between logs
- Repetitive unsuccessful logon attempts within a short time interval
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system files
- Denial/disruption of service or inability of one or more users to login to an account
- Unusual time of usage (e.g. users login during unusual times)
- Unusual system resource consumption. (High CPU usage)

- Operation of a program or sniffer device used to capture network traffic
- . Unauthorized changes to user permission or access

Phase 3

Containment requires a reasonable understanding of the incident and the means by which to combat that incident. IRO-2 will be tasked with the critical-decision making process to address and contain potential threats. Some methods they may use include:

- Enable disposable Administrative accounts for use during the investigation
- Attempt to isolate the invading code
- Preserve evidence as much as possible
- Avoid changing volatile or system state data
- Identify and harden security around critical systems and services (i.e. email, DNS, service applications
- Conduct packet capture (i.e. Wireshark, etc…)
- Monitor potential communication channels being used by the attacker

Phase 4

Elimination of threat is crucial to getting the system back to its initial state. The following may be done to eliminate malicious threats

- Presentation Layer
  - Remove insertion points within the application so that code injection is less possible.
  - Disable active sessions from infected user(s) on the web application
  - Lock user’s account if credentials are being used.
- Business Layer
  - Closed unnecessary ports
  - Increase authentication security parameters
- Database Layer
  - Limit/Restrict data manipulation.
  - Setup notifications of unauthorized attempts of data manipulation.

Phase 5

Upon ensuring the systems are free of malicious code injection, it is time to restore the network services. The IRO-2 will authorize restoration efforts for the application. These include but are not limited to:

- Restoring services from a clean back up
- Replacing corrupted data from a clean back
- Restoring network connections
- Increase monitoring activities
- Implement a 3rd party support element to help detect or prevent future attacks

Phase 6

As network attacks are far more likely than most other incidents, it is crucial that a full detail of events is recorded and logged for evaluation. The IRO-2 will be tasked with created such a log and report. These elements include, but are not limited to, the following:

- All system events (audit records, logs)
- All actions taken (including the date and time that an action is performed)
- All external conversations
- Investigator Notes compiled
- Any deviations from SOP and justifications
- A description of the exact sequence of events
- The method of discovery
- Preventative measures put in place
- Assessment to determine whether recovery was sufficient and what other recommendations should be considered

Acknowledgements

Wellness Technology is a company that prides itself on being a leader in technology, but we also take being ethical in our approach to creating guides and procedures. This document was no different in that approach. Knowing our corporate structure, we were able to glean some our response efforts based on models of our industry colleagues. FP Secure and the University of Texas Medical, we thank you.

References

FP Secure. (2020, September). *FRSecure Security Incident Management Plan Template.* https://frsecure.com/resource/incident-management-plan-template.pdf

University of Texas Medical Branch. (2017, November 7). *Fire Alarm and Incident Response Policy*. https://www.utmb.edu/policies_and_procedures/IHOP/Health_Safety_and_Security/IHOP%20-%2008.01.05%20-%20Fire%20Alarm%20and%20Incident%20Response%20Policy.pdf