**U09A1 – Business Continuity Management Plan**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4076: Security Management and Policies

Stuart McCubbrey

June 2023

1. **Overview**

The Business Continuity Management Policy (BCMP) establishes the necessary policies and procedures to ensure uninterrupted business operations during significant disruptions, it encompasses both physical and logical aspects for the organization, focusing on the critical systems required for day-to-day activities.

* 1. **Purpose**

The purpose of this policy is to minimize the organizational downtime by implementing effective policies and procedures. High Class Healthcare aims to respond quickly and efficiently to all incidents, restoring normal working conditions quickly. The policy covers all areas of the organization by emphasizing its commitment to providing exceptional patient care and community outreach.

* 1. **Scope**

This policy applies to all individuals associated with High Class Healthcare including employees, volunteers, and contractors. The policy will ensure that all parties associated with High Class Healthcare understand and adhere to the requirements for business continuity.

1. **Policy**

There are several parts to a Buisness Continuity Management Plan (BCMP) that include obtaining a risk assessment and analyzing the impact of the risk to the business. From these two policies the BCMP will be able to better plan and manage a disaster recovery with the Disaster Recovery Plan and Incident Response Plan.

Training and awareness will be provided yearly to all employees, vendors, contractors, and any entity that works with High Class Healthcare. This will ensure that all individuals associated with the organization know and understand what is required for business continuity. Flyers and info graphics can be placed around the hospital in employee breakrooms and offices reminding them of the importance of security awareness.

* 1. **Risk Assessment**

Before a Disaster Recovery Plan can be completed a risk assessment must be developed. The risk assessment will follow the guidelines set by NIST SP800-37r.2 for how to assess risk the likelihood of the risk. The risk assessment will help High Class Healthcare to understand what systems and resources are vital to the day-to-day operations. The risk assessment will consider both internal and external threats. These threats can be in the form of cybercrime, natural disasters, and human disasters.

The risk assessment will define individual responsibilities associated with security and privacy risk management. The risk assessment will establish a strategy that includes determination of the possible risks that could occur and the organization’s ability to tolerate that risk. The risk assessment will also include strategies on how to reduce the impact of the risk. This can include mitigation, risk transfer or avoidance, and risk acceptance or reduction.

The risk assessment must be able to crosswalk to OSHA, HIPAA, SOX, and PCI-DSS regulations.

There are 5 steps that must be defined in the policy:

1. Identify hazards.
2. Evaluate the risks.
3. Define control measures.
4. Document the findings.
5. Review, assess, and update policy as needed.
   1. **Buisness Impact Analysis (BIA)**

The Business Impact Analysis will help to define the impact of different types of disruptions that could occur. The BIA will use the Risk assessment to understand what systems and devices are vulnerable and at risk due to disruptions to daily operations. This will include both natural and human disasters. The policy will define the most critical areas that must be protected and their dependencies.

To better understand the impact on the organization the BIA will consider the impact to the financial, operational, relational, and legal impacts due to a disruption. High Class Health care can use two measurements to better understand the impact: Recover Time Objective (RTO) and the Recovery Point Objective (RPO). Using the RTO the organization can find the maximum amount of down time determined to assess the cost impact on the organization. The RPO is defined as the max amount of time that critical data can be down before it becomes a major disruption to business. Then using the RPO the organization will be able to determine how often data backups must be done.

* 1. **Disaster Recovery Plan (DRP)**

A properly formed DRP will ensure all data is recoverable and there is limited to no loss of data integrity.

The DRP will outline how the organization will bring systems back online to ensure the least amount of disruption to daily activity. The DRP must have 4 elements included in the policy: RTO, scope, identification of team members, and escalation details. This policy will help to reduce the RTO such that there is little to no disruption in day-to-day operations. The DRP will classify the assets that need protecting such as IT systems, data, and employees with high knowledge skills.

Regular tests must be conducted on the organizations systems and network to assess any new holes. There are several tests that can be conducted. Table tests should be conducted quarterly, simulation tests done twice a year, and full interruption testing done every 2 years.

Using FIPS 199 the organization will be able to classify the assets according to the level of risk to confidentiality, integrity, and availability. This will include Personally Identifiable Information (PII) and Protected Health Information (PHI) that aligns with regulatory requirements defined by HIPAA. Once data and asset inventory has been classified

* 1. **Incident Response Plan (IRP)**

The IRP is designed to be aligned more with data protection than the DRP. A properly designed IRP will have a coordinated and timely response to security incidents, that will include reporting, containment, mitigation, and recovery. There will be different IRPs created for different areas of the buisness that can be affected by the attack. There needs to be compliance written into the policy that takes into effect defined security breach notification requirements such as HIPAA, SOX, PCI-DSS. In this policy an alternate site (hot, warm, cold) will be defined. There are 5 components that must be included in this policy.

1. Proper step-by-step instructions on how to proceed during an incident.
2. Data flow diagrams that map out how the data is moved around.
3. Network diagrams that map out how the network is connected.
4. System configuration details that define how each system is configured.
5. An incident call list that defines who to call when an incident occurs. Such as CIO, Legal team, and IRP team contact.
   1. **Post Incident Reviews (PIR)**

The PIR will take into consideration who was impacted, which systems were affected, and what data has been impacted. This can be done through interviews, logs, and internal forensic searches. The PIR will help to identify what systems can be automated to reduce the workload on the IT security team. The organization may also create and use a playbook that can help to weed out false negatives and correlate security alerts to pinpoint areas of attack.

Yearly reviews will be conducted through a 5-step process after a disaster recovery is performed to assess how the organization was affected, what the organization will do to prevent the disaster, and how it will incorporate the new designs into the BCMP.

There are 5 steps to the PIR to ensure the BCE continues to remain effective and relevant now and in the future.

1. Review Business Impact Assessment – Review BIA for and ensure it is up to date and relevant to today’s risks.
2. Conduct a risk assessment. – document and analyze any changes made since the previous review
3. Review risk reduction strategies – Weigh current reduction strategies with OWASP top 10 current risks and vulnerabilities.
4. Evaluate BCE effectiveness – Ensure BCE is current and up to date. All systems, data, and network are prepared for any new disasters.
5. Complete training and awareness communication – Ensure that training and awareness campaigns are updated to the latest security strategies.
6. **Policy Compliance**

All employees, contractors, vendors, and volunteers must comply with this Operational Management Security Policy, Failure to follow this policy will result in disciplinary action, up to and including termination of employment, services, or contracts.

If any violation of this policy is seen it must be reported to either the IT security department or to the department manager of your assigned department for further investigation or escalation.

1. **Roles and Responsibilities**

Roles and Responsibilities are assigned to current positions within High Class Healthcare.

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| CEO | Oversee and authorize final approval of any changes made to this policy.  Provide leadership and guidance to team members and other stakeholders.  Ensure the development, implementation, and maintenance of the policy. |
| CIO | Review and update policy every year |
| Network Administrator | Ensures that systems and data are reconnected as per policy details |
| IT Security | Recommends and appends network security ensuring transition to and from disaster is smooth |
| Help Desk Supervisor | Informs and educates departments in hospital of and IT changes needed to ensure business continuity |
| All employees, contractors, vendors, and volunteers | Read, understand, and follow all policy guidelines. |

1. **Related Standards, Policies, and Processes**

NIST SP800-37r.2

FIPS 199

HIPAA

OWASP Top 10

SOX

PCI-DSS

1. **Definitions and Terms**

CEO – Chief Executive Officer

CIO – Chief Information Officer

C-I-A – Confidential, Integrity, and availability. Refers to ensuring sensitive information is safe, secure, and available to authorized entities only.

RTO - Recover Time Objective is the maximum tolerable length of time systems can be down after a failure.

RPO – Recovery Point Objective is the maximum amount of time that critical data can be down before it becomes a major disruption to business.

1. **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Summary of Changes | Approval |
| 1.0 | 06/10/2023 | Creation of new policy | Mark Moneybags, CEO |