MAJOR IT INCIDENT RESPONSE PLAN

BE PREPARED

An IT failure can be costly to your business, customer privacy, and financial assets. Protect your business, and the substantial investment in your IT infrastructure, by having a plan in place. It is never a good idea to wait until disaster strikes.

MAJOR IT INCIDENT DEFINITION

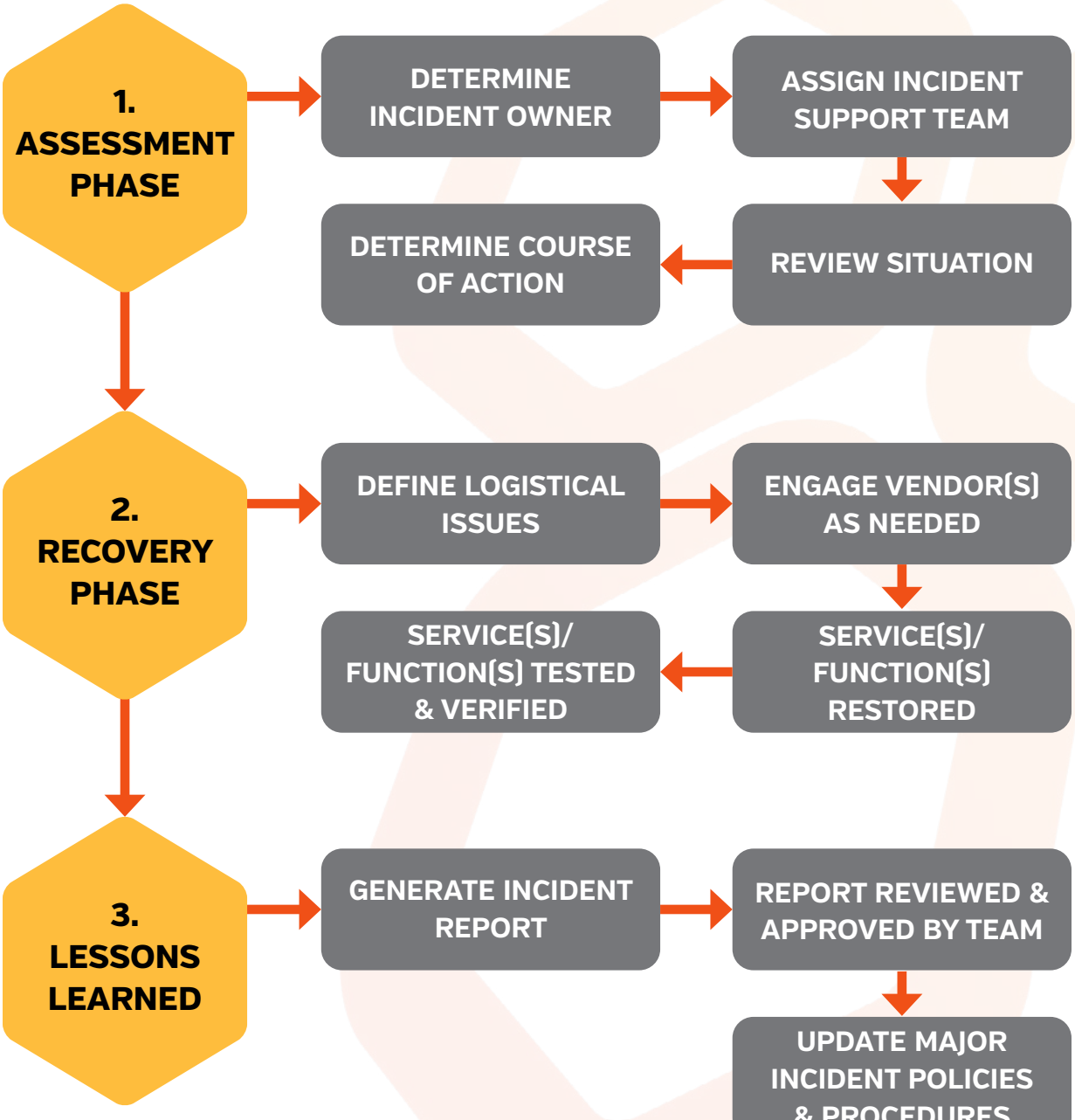
A Major IT Incident is defined as a total failure (all users equally affected) of one or more core services, functions, or devices. After exhausting basic troubleshooting, a Major IT Incident is declared if it meets one or more of the following criteria.

A Major IT Incident may include, but is not limited to:

- **A total failure of any core business application**
  - Examples:
    - Microsoft Exchange
    - Microsoft Active Directory
    - Microsoft SQL
    - Microsoft Hyper-V
    - VMWare\ESX
    - Line of Business Applications (e.g. SAGE 300, Timberline, Tap.)
- **Significant loss or potential loss of data**
  - Examples:
    - Crypto Malware Infection
    - Network Security Breach
    - Failed Hardware
    - Theft of device or data

- **A total failure of any core business service (Not ISP related)**
  - Examples:
    - Complete loss of VoIP function
    - Complete loss of Internet connectivity
    - Complete loss of remote access
    - Complete loss of access to web-based assets
- **Prolonged ISP outage (More than 4 hours)**
- **A total failure of one or more production devices**
  - Examples:
    - Physical Server - down hard
    - Virtual Server - down hard
    - Storage Array \ SAN - down hard
    - Network Switch\Router\Firewall - down hard

MAJOR IT INCIDENT RESPONSE PLAN



ASSESSMENT PHASE

- **Key leadership personnel are called together to discuss and review the issue and decide course of action.**
- **Incident Owner is established.**
  - The Incident Owner will be the primary team member responsible for performing, facilitating, and tracking necessary work to resolve the Major Incident to completion. This includes any off hours work and follow up with vendors, and any other stakeholder. The Incident Owner will track the Major Incident and communicate any status updates to leadership and Incident Support Team when new information becomes available, or at an agreed upon interval. The Incident Owner may transfer communication responsibilities to the Incident Support Team if necessary. The Incident Ownership may be transferred with valid cause and agreement of all parties.
- **Incident Support Team is established.**
  - The Incident Support Team will be responsible for assisting the Incident Owner in resolving the incident. The Incident Support Team will consist of one or more team members and should include a senior team member. The Incident Support Team will provide escalation, logistical, and any other needed support to the Incident Owner.
- **A channel of communication is established between key personnel (Slack®, Teams®, Email, etc.)**
  - Incident Owner to set reminder for interval or established check in time.
    - Not needed if no specific interval is established
  - Status indicators to be used in communications:
    - WIP – Work in Progress
    - RP – Resolution Pending
    - RC – Resolution Confirmed

RECOVERY PHASE

- **Incident Owner works to resolve the issue.**
- **Incident Owner engages Incident Support Team as needed for:**
  - Logistical issues
  - Ability\Knowledge issues
  - Vendor engagement
- **Upon resolution**
  - The Incident Support Team validates issues are resolved and all services, applications, devices are functioning normally, security issues have been resolved and data is restored to the fullest extent possible.

LESSONS LEARNED PHASE

- **A Major Incident Report is generated by the Incident Owner detailing:**
  - Overview of issue(s)
  - Summary of key steps to resolve including decisions\ communications with primary contact(s)
  - Timeline of events
  - Root cause of issue
  - Recommendations
- **Report is reviewed by the Incident Support team for overall accuracy, level of detail, and recommendations.**
- **Incident Owner presents report to leadership team and reviews with them.**
- **Report is reviewed by all team members to identify if any changes to the Major Incident Response Policy and Procedure are necessary.**

IN-HOUSE SOLUTIONS VS. OUTSOURCED IT SOLUTIONS

When your staff devotes the majority of their time to keeping everything running, little time remains for projects that could boost internal operations, improve client service and support new business opportunities. Add in a major IT incident and your crucial team is on overload.

That's where FUSE3 comes in. We are well-versed in emergency situations and how to properly and efficiently respond to any Major IT Incident. Focus on what you do best and rest assured that FUSE3 will work with you to keep your systems functioning securely and at the highest level.

CONTACT US TODAY

FUSETHREE.COM | FUSE3