Inject Number: 18

From: Team X

To: CIO

Subject: Pres: Disaster Recovery Plan

CIO,

The following is our disaster recovery plan that you’ve requested.

Reference Used: Microsoft Premier Field engineers Disaster Recovery Planning, <https://blogs.technet.microsoft.com/mspfe/2012/03/08/a-microsoft-word-document-template-for-disaster-recovery-planning/>

Regards,

-Team X

**Disaster Recovery Plan**

# Overview

CCDC developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the features listed in the table above. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

# Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by CCDC that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

# Scope

The scope of this DRP document addresses technical recovery only in the event of a significant disruption.

# Policy

**Data loss/disruption:** In the event of data loss/disruption, the disaster recovery team will restore data from backups. Backups are scheduled to run daily at multiple times to ensure minimal loss of data. During a disruption, operations may run at a reduced rate. The following are steps that will be taken in the event of data loss or a disruption in service:

1. Issue is identified, team is alerted of the pending issue, issue is communicated/escalated.
2. Team members are identified for recovery roles, members prepare for restoration phase.
3. Communication to other teams is established. (phone, email, etc.)
4. Recovery strategy/method is established, estimated time duration is calculated.

Our most critical items are customer/user data as well as systems that keep our business operational.

**Prevention:** Security/IT Staff will monitor system status and make changes to increase system security as necessary. Security staff will re-evaluate our current security implementation and communicate any changes to the appropriate teams. Staff will continuously monitor network traffic to make sure future attacks are prevented.

**Data Recovery:** In the event of a security breach, the disaster recovery team will immediately restore data from backups. The security/IT Staff may temporarily block all incoming access to our systems while this restoration process is taken place to prevent further damage. Security/IT staff will immediately make changes to the network firewall to prevent the same attack from reoccurring. Once data is restored, our systems will be brought back online to resume normal operations.