

NOTE: This template contract is freely shared by SecurityStudio. Any/all modifications of this document are permitted; however, we request this template be shared freely with others in our attempt to help them with their information security challenges too. Everything we do at SecurityStudio is focused on our mission; *to fix the broken (information security) industry*.

**#MissionBeforeMoney**

INSTRUCTIONS: Modify all parts of this document to fit for your organization, including changing logos, format, and/or language. The most common mistake when using a template like this is to not reflect the culture of your organization. Replace all “(ORGANIZATION)” tags with your organization’s name.

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](http://creativecommons.org/licenses/by-sa/4.0/).

Ransomware Recovery Contract

To ensure proper accountability in the protection of (ORGANIZATION) operations during and after a ransomware attack.

# Purpose

(ORGANIZATION) is committed to protecting its information and the information entrusted to it by customers and partners. (ORGANIZATION) recognizes the threat posed to its operations by ransomware, and to this end has adopted this contract to ensure accountability is understood and agreed upon by responsible parties.

This contract should provide assurance to stakeholders that (ORGANIZATION) can restore operations in the event of a ransomware infection **WITHOUT** paying a ransom to criminal attackers.

# Precautions

The following precautions have been taken to protect and restore operations at (ORGANIZATION):

[ ] Backups of all critical files and file systems are taken no less frequently than daily.

[ ] Important data on PCs is backed up on a monthly basis (or more frequently).

[ ] Weekly (or more frequent) backups are stored online **and** offline (not network connected).

[ ] Restoration testing, including the restoration of entire servers, is done on a quarterly basis (or more frequently).

[ ] Backups are verified as restorable.

[ ] Personnel do not have administrative privileges on workstations/laptops.

[ ] Personnel do not use administrative accounts for daily work activities.

[ ] Domain Accounts and Groups are monitored for changes, including privilege escalation.

[ ] All personnel are informed about how to report ransomware, or what may appear to be ransomware.

**Exceptions to the above precautions include:**

**NOTE: Any exceptions should be accompanied by a separate acceptance by management or workorder for completion.**

# Signatures

I attest to the accuracy of the information contained within the section titled “Precautions”.

|  |
| --- |
| **Information** **Technology** |
| **Name** |  |
| **Signature** |  |
| **Date** |  |

I understand that the basic precautions, as noted above, will allow (ORGANIZATION) to restore operational disruptions caused by ransomware in most cases. I also understand the impossibility of guaranteeing the organization will be able to restore operations in a timely manner, in all circumstances.

|  |
| --- |
| **Executive Management** |
| **Name** |  |
| **Signature** |  |
| **Date** |  |