zetta Ransomware Prevention Checklist

Immediate Steps to Take After a Ransomware Attack

- **Disconnect infected machine from the network & Internet** — so ransomware doesn't spread to other machines
- **Run a virus scanner from a bootable disc or USB drive** (aka an offline virus scan) — to try to remove the virus from the machine
- **Do a System Restore** — this takes your machine back to a previous state (this option is in earlier versions of Windows (pre Win 8))
- **Reformat the hard drive and reinstall your last backup**

How to Prevent Future Ransomware Attacks

Review & Update Network Security

- Keep Windows Firewall on at all times if you run Windows
- Install an anti-virus program that has a real-time virus scanner and automatically updates
- Keep your browser and plug-ins up-to-date, including Adobe Flash Player, Java, etc.
- Keep up-to-date inventory of all of your digital assets, so hackers don't attack systems you're unaware of
- Segment your file access so only authorized users have permission to make changes
- Install pop-up blockers, since pop ups are another entry way for ransomware viruses

Ensure Data & Hardware Are Adequately Protected

- Keep your OS and applications up to date
- Back up your critical data on a regular basis — so if you're a victim of ransomware, you can recover your important data without being forced to pay up
- Always have a copy of your data offsite — whether on an external hard drive, secure cloud, or best case scenario: both

Change Online Behaviors & Practices

- Never download attachments from unknown senders or sources you don't know
- Don't download and execute unauthorized applications from the Internet unless they are from a trusted source and have been scanned for malware