



TEMPEST RISK MANAGEMENT

Tempest Risk Management LLC

CyberSecurity Policy Template

2022

Authored by Andy Ziegler, CBCP

CyberSecurity Policy Template			
Company Name:	Company XYZ		
Version #	1	Revision Date	Feb 2022

PURPOSE

Keeping our data and cyber infrastructure is critical to being able to serve our clients and protect their information and privacy. This policy must be followed by all employees at all times.

APPLICABLE ROLES

All employees

CYBERSECURITY POLICY TEMPLATE

All employees must follow the cyber security policy outlined below. Failure to follow basic IT/Cyber security hygiene practices may result in disciplinary action

1. **Strong passwords** – Passwords must be at least 10 characters and use a combination of lowercase and uppercase letters, numbers and special characters
2. **Password rotation** – Passwords must be changed every 90 days for critical and data sensitive systems
3. **Multi factor authentication** – whenever available, enable multi factor authentication for access to systems or services.
4. **Never share passwords.** If a password must be shared in an emergency, gain permission from your immediate supervisor first and change the password immediately following the emergency.
5. **Never access company systems via public internet.** Always use private, secured internet access.
6. **Never click on suspicious links** received via email or found on the internet.
7. Never download or open files from unconfirmed or unexpected sources.
8. Always check email and names for suspicious content. Look for inconsistencies, poor grammar, strong/threatening call to action such as clicking on a link to login to a bank account.
9. **Acceptable Use** – Company systems, equipment and internet access is only to be used for legitimate company business purposes.
10. **Installation** of hardware, software or cloud based API's must be approved by the IT department or your immediate supervisor before being placed into service.
11. **Always lock** all devices (computers, phones, etc) when not in use.
12. **Ensure recipients of data** are properly authorized people or organizations with adequate security policies and proper legal agreements in place.
13. **Report any cyber security concerns** immediately to IT or your immediate supervisor including:
 - a. Potential security breach by you or another employee
 - b. Out of date anti-virus/malware software
 - c. Out of date browsers, operating systems or other software requiring updates
 - d. Compromised username or password
 - e. Targeted phishing (fake emails) smishing (fake text messages) or any suspected attempt at social engineering

More information on cyber security practices can be found at <https://americassbdc.org/cybersecurity>

WHERE DO YOU STORE YOUR POLICIES AND PROCEDURES?
CAN YOUR EMPLOYEES EASILY ACCESS THEM AT ALL TIMES?

MANANGE YOUR OPERATIONS

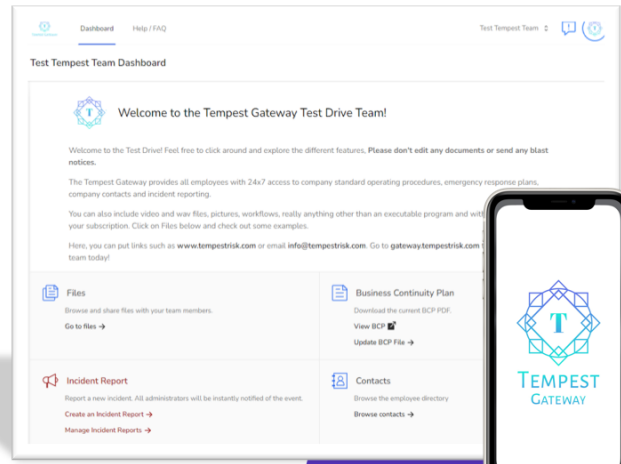
Tempest Gateway

The Tempest Gateway is a **User Friendly & Customizable** mobile operations platform for your business.

With a web interface and companion mobile apps, your business is always in the palm of your hand.

SOP & Document Storage, Interactive Employee Directory, Customizable Dashboard, Incident Reporting, and so much more!


gateway.tempestrisk.com



Operational Resilience Solutions

At Tempest, we specialize in improving business operations by identifying our clients needs and helping them become more resilient.

3 Ways to Improve Operational Resilience:

-  Tempest Gateway Ops Platform >
-  Business Continuity Planning >
-  SOP's and Operations Manuals >



Email Us

info@tempestrisk.com



Call Us

(302) 598-8027



Schedule Meeting

[Pick a Date & Time](#)

