Cybersecurity Preparedness Plan

[Company Name and Date]

An overview of the business and its critical assets and data	This section should provide a brief description of the business, its operations, and the sensitive information and assets that need to be protected.
A list of security policies and procedures	This section should outline the security policies and procedures that have been developed to protect the business from cyber threats. This may include guidelines for creating strong passwords, using encryption, and avoiding phishing scams.]
Employee training and awareness	This section should describe the training and awareness programs that have been implemented to educate employees on the importance of cybersecurity and how to stay safe online.
Technical controls	This section should describe the technical controls that have been implemented to protect the business from cyber threats. This may include firewalls, antivirus software, intrusion detection systems, and other security measures.
Incident response plan	This section should outline the steps that will be taken to respond to a security incident, such as a hacking or ransomware attack. This plan should include contact information for key personnel, procedures for backing up data, and instructions for reporting the incident to the authorities.
Ongoing monitoring and review	This section should describe the processes and procedures for monitoring the effectiveness of the cybersecurity plan and conducting regular reviews to ensure that it remains up to date and effective. This may include regular audits, risk assessments, and updates to security policies and procedures.