

Cybersecurity Policy

1. Introduction

Throwe Environmental is committed to maintaining the highest standards of cybersecurity to protect sensitive information associated. This policy outlines the measures implemented to safeguard our data and technology assets.

2. Scope

This policy applies to all employees, contractors, and partners who have access to Throwe Environmental's data and technology systems.

3. Data Storage and Management

Secure Data Storage.

We utilize Google Drive for secure data storage and management. Google Drive provides robust security features including encryption at rest and in transit.

Access Control.

Access to Google Drive is restricted to authorized personnel only. Permissions are granted based on the principle of least privilege, ensuring that individuals only have access to the data necessary for their role. Upon a team member's departure (voluntary or involuntary) from Throwe Environmental, permissions are appropriately rescinded to prevent legacy access issues.

4. Authentication and Access

Two-Factor Authentication (2FA).

We enforce 2FA for all accounts accessing our data storage systems. This adds an additional layer of security by requiring a second form of verification beyond just a password.

Strong Password Policies.

All users must create strong, unique passwords and change them regularly. Passwords must not be shared or reused across multiple accounts.

5. Data Encryption

Encryption Protocols.

All sensitive information is encrypted using industry-standard encryption protocols. This ensures that data remains confidential and secure during storage and transmission.

Email Encryption.

We utilize end-to-end encryption for email communications involving sensitive information to prevent interception by unauthorized parties.

6. Data Backup and Recovery

Regular Backups.

Regular data backups are performed to prevent data loss in the event of a system failure or other unforeseen incidents.

Recovery Procedures.

Our data recovery procedures are tested periodically to ensure quick and effective restoration of data when necessary.

7. Device Security

Device Management.

All company devices must be secured with passwords, encryption, and anti-virus software. Devices should be kept up-to-date with the latest security patches.

Remote Work Security.

Employees working remotely must ensure their home networks are secure, using strong passwords and updated firmware on routers.

8. Incident Response

Incident Reporting.

All employees must report any suspected security incidents immediately to the IT department.

Response Plan.

We have a defined incident response plan to address and mitigate the impact of security breaches.

9. Training and Awareness

Employee Training.

Regular cybersecurity training sessions will be conducted to ensure all employees are aware of current threats and best practices.

Security Awareness.

Ongoing awareness campaigns will be implemented to keep cybersecurity top-of-mind for all employees.

10. Compliance and Monitoring

Regulatory Compliance.

We adhere to all relevant data protection laws and regulations, including GDPR and HIPAA.

Regular Audits.

Regular security audits and assessments will be conducted to identify and mitigate vulnerabilities in our systems.

11. Third-Party Vendors

Vendor Security.

All third-party vendors must comply with our cybersecurity standards. Contracts will include specific security requirements and regular compliance checks.

12. Continuous Improvement

Feedback Mechanisms.

Employees are encouraged to provide suggestions and feedback on cybersecurity practices. This input will be used to continually refine and improve our security measures.

Regular Assessments.

Throwe Environmental will conduct regular assessments of its cybersecurity practices, measuring progress against defined goals and making adjustments as needed to align with emerging best practices.

This Cybersecurity Policy is a reflection of Throwe Environmental's commitment to protecting our data and technology assets. By adopting robust security measures, promoting awareness, and engaging in continuous improvement, we aim to safeguard our organization and our stakeholders' information.

APPROVED BY:



Joanne M. Throwe
President
Throwe Environmental, LLC

UPDATED 08/05/2024