Marshall Creative Cybersecurity Policy

1. Purpose and Scope

Marshall Creative recognizes the critical importance of cybersecurity in safeguarding our digital assets, protecting sensitive information, and ensuring the continuity of our operations. This Cybersecurity Policy establishes the framework for implementing and maintaining effective cybersecurity measures.

2. Cybersecurity Objectives

- Confidentiality: Ensure the confidentiality of sensitive information by preventing unauthorized access, disclosure, or theft.
- Integrity: Protect the integrity of our digital assets by preventing unauthorized alterations, modifications, or destruction.
- Availability: Ensure the availability of our digital resources and services by protecting against disruptions, denial-of-service attacks, and other cyber threats.

3. Compliance with Cybersecurity Standards

Marshall Creative is committed to complying with recognized cybersecurity standards, frameworks, and best practices. This includes adherence to ISO/IEC 27001, NIST Cybersecurity Framework, and any other relevant industry-specific standards.

4. Risk Assessment and Management

Regular cybersecurity risk assessments will be conducted to identify and assess potential threats and vulnerabilities. Mitigation strategies will be implemented to address these risks and ensure the ongoing resilience of our digital infrastructure.

5. Network Security

Implement and maintain robust network security measures, including firewalls, intrusion detection and prevention systems, and regular monitoring to safeguard against unauthorized access and malicious activities.

6. Endpoint Security

Ensure the security of all endpoints, including computers, mobile devices, and other connected devices. Implement endpoint protection solutions, encryption, and regularly update security patches.

7. User Authentication and Access Controls

Implement strong user authentication mechanisms and access controls to ensure that only authorized individuals have access to specific systems, applications, and data.

8. Incident Response Plan

Establish and maintain a comprehensive incident response plan to effectively respond to cybersecurity incidents. This plan will include procedures for reporting incidents, containment, eradication, recovery, and communication.

9. Employee Training and Awareness

Regularly train employees on cybersecurity best practices, recognizing social engineering tactics, and staying vigilant against phishing attacks. Foster a culture of cybersecurity awareness and responsibility.

10. Encryption

Implement encryption protocols for sensitive data in transit and at rest. This includes data stored on servers, databases, and any data transmitted over internal and external networks.

11. Regular Security Audits and Assessments

Conduct regular security audits and assessments to identify vulnerabilities, assess the effectiveness of existing security controls, and implement improvements based on findings.

12. Secure Software Development Practices

Incorporate secure coding practices into software development processes to mitigate vulnerabilities and reduce the risk of introducing security flaws into applications.

13. Vendor Security Management

Ensure that third-party vendors and service providers adhere to cybersecurity standards compatible with our own. Contracts with vendors will include cybersecurity requirements and regular assessments.

14. Continuous Monitoring and Improvement

Marshall Creative is committed to continuous monitoring of our cybersecurity posture and will regularly update and improve security measures to adapt to evolving threats and technologies.

15. Review and Revision

This Cybersecurity Policy will be reviewed periodically to ensure its continued relevance and effectiveness. Necessary revisions will be made to adapt to changes in cybersecurity threats, regulations, and industry best practices.

This Cybersecurity Policy reflects Marshall Creative's dedication to maintaining a robust cybersecurity posture, protecting digital assets, and minimizing the impact of cyber threats on our operations and stakeholders.

Signed
Darren Marshall [DIRETCTOR]

21st Jan 2024