The Walt Disney Company

TWDC INFORMATION SECURITY MANAGEMENT SYSTEM

PURPOSE:

This document outlines The Walt Disney Company ("TWDC") approach to Information Security.

BACKGROUND:

TWDC follows a number of Information Security best practices and frameworks including COBIT, CIS, ISO 27001, PCI-DSS, NIST 800 series and ITIL to manage Information Security Risk.

To support a common understanding of TWDC's Information Security practices, this document applies the U.S. National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity version 1.1 (known as the "NIST Cybersecurity Framework") to describe TWDC's approach.

NIST CYBERSECURITY FRAMEWORK ALIGNMENT

The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity. The framework outlines twenty-three groups of cybersecurity outcomes aligned to a Framework of Core activities (Identify, Protect, Detect, Respond, and Recover). This document leverages these groups of cybersecurity outcomes to describe publicly TWDC's approach to Information Security.

Identify: Asset Management

TWDC data, personnel, devices, systems, and facilities are identified through a combination of manual processes and automated enumeration tools and techniques. High impact systems are categorized, and data is classified as confidential, internal use, or public.

Identify: Business Environment

TWDC employs Information Security Officers across the Enterprise who align cybersecurity activities with the organization's mission, objectives, and stakeholder needs.

Identify: Governance

TWDC has chartered an organization-wide Information Security Committee that continually reviews, updates and publishes policies, standards, and guidelines to address the Company's regulatory, legal, risk, environmental, and operational needs.

Internal and external assessors periodically evaluate the Company's information security program from both a design and effectiveness perspective.

Identify: Risk Assessment

TWDC measures, assesses, and reports on cybersecurity risks at a system, operational, program, and strategic level.

Identify: Risk Management Strategy

TWDC periodically assesses the Company's risk tolerance and has established risk principles that are used to drive both policy and operational risk decisions. Additionally, TWDC obtains insurance against the risk of losses relating to some technology events.

Identify: Supply Chain Risk Management

TWDC has a comprehensive vendor management program, including performing due diligence assessments and leveraging legal contracts, to manage third-party supply chain risk.

Protect: Identity Management, Authentication and Access Control

TWDC implements host- and network-based controls to limit access to physical and logical assets and associated facilities to authorized users, processes, and devices. Logical access leverages two-factor authentication to reduce the risk of unauthorized access.

Protect: Awareness and Training

TWDC provides regular cybersecurity awareness and education to the Company's personnel and partners. Additionally, employees receive cybersecurity policy training as part of the training related to compliance with the Company's standards of business conduct.

Protect: Protect Data Security

TWDC protects the confidentiality, integrity, and availability of information with a combination of access controls, encryption controls, and backup and recovery controls. Data is protected in line with the Company's data classification scheme.

Protect: Information Protection Processes and Procedure

TWDC protects information with formal Records Information Management, Data

Security, and Content Protection programs.

Protect: Maintenance

TWDC performs maintenance and repairs of information system components consistent with Company's change and configuration management policies and procedures.

Protect: Protective Technology

TWDC manages a number of host- and network-based controls to protect against malware, hacking, social, physical, misuse, human error, and environmental threats.

Detect: Anomalies and Events

TWDC deploys host- and network-based technology to detect anomalous activity and understand the potential impact of events.

Detect: Security Continuous Monitoring

TWDC deploys host- and network-based technology to monitor information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures.

Detect: Detection Processes

TWDC centrally maintains and periodically tests detection processes and procedures.

Respond: Response Planning

TWDC administers a centrally-managed formal incident response plan.

Respond: Communications

TWDC administers a centrally-managed formal incident response program that coordinates all response activities including communication.

Respond: Analysis

TWDC administers a centrally-managed formal incident response program that coordinates all response activities including analysis.

Respond: Mitigation

TWDC administers a centrally-managed formal incident response program that

coordinates all response activities including mitigation.

Respond: Improvements

TWDC administers a centrally-managed formal incident response program that coordinates all response activities including after-action reviews and lessons learned.

Recover: Recovery Planning

TWDC maintains disaster recovery plans for systems deemed mission critical to the Company. Additionally, TWDC obtains insurance against the risk of losses relating to some technology events.

Recover: Improvements

TWDC periodically tests and improves disaster recovery plans for systems deemed mission critical to the Company.

Recover: Communications

TWDC maintains disaster recovery plans for systems deemed mission critical to the Company. These plans are fully integrated with TWDC's crisis management communication protocols.