Comcast[1] Cybersecurity

Information Security Program Summary

Updated: July 2022

[1] Includes Comcast Corporate and Comcast Cable and its subsidiaries, but excludes any other Comcast Corporation subsidiaries, including NBC and Sky.

Table of Contents

Introduction

This Information Security Controls Policy provides a summary of our information security program at Comcast.

The document is for use with customers who are engaging Comcast to provide services and who have questions on our information security program.

This Information Security Controls Policy is current at the time of issue and is reviewed annually.

Security Commitment

At Comcast, risk management, including the safeguarding of customer information, is very important. We are committed to meeting our obligations under data privacy laws and regulations in each of the areas in which we do business. Information security is a core business concern and our internal controls, information technology risk management and data privacy programs are designed to achieve our risk management objectives.

Comcast's Information Security Program aligns with NIST 800-53, PCI and ISO 27000. Our Cybersecurity program is designed to:

- Protect customer information
- Monitor systems, protect them against viruses and other threats, and enable them to recover quickly from incidents
- Perform information security risk assessments to analyze, identify, evaluate, prioritize and remediate risk
- Require that our key third-party service providers adhere to specific security policies and standards, as well as regulatory obligations as applicable
- Maintain ongoing audits of control procedures to ensure optimization of environments to prevent unauthorized information access or disclosure
- Educate employees to understand their responsibilities with respect to the protection of customer information and security of our systems preventing breaches

Comcast has developed policies, standards, procedures or practices regarding the issues described below, as appropriate.

Cybersecurity Policy

Objective	Action
Providing management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations.	A set of policies for cybersecurity has been defined, approved by Comcast Cable management, published, and communicated to employees and relevant external parties.
	The policies for cybersecurity are reviewed at planned intervals, or if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.

Cybersecurity Program

Objective	Action
Establishment of a management framework to initiate and control the implementation and operation of cybersecurity within Comcast Cable.	An enterprise cybersecurity program exists within Comcast Cable which governs the protection of information and data against loss or misuse.
	Definition and allocation of cybersecurity responsibilities.
	Segregation of conflicting duties and areas of responsibility.
	Establishment and maintenance of appropriate contacts with relevant authorities.
	Establishment and maintenance of appropriate contacts with special interest groups or other specialist security forums and professional associations.
	Inclusion of cybersecurity in project management, regardless of the type of project.
	Regular review of Comcast Cable's goals and objectives for cybersecurity.

Human Resources Security

Objective	Action
Understanding responsibilities and suitability for roles.	Review of personnel background in accordance with relevant laws, regulations, and ethics, and are proportional to the risk posed by the role.
	Inclusion of contractual responsibilities for cybersecurity in agreements.
Awareness of cybersecurity responsibilities.	Requirements to apply cybersecurity in accordance with the established policies and procedures of Comcast Cable.
	Provision of appropriate awareness education and training and regular updates regarding Comcast Cable's policies, standards, and procedures, as relevant to their job function.
Protection of Comcast Cable's interests as part of the process of changing or terminating employment.	Definition and communication of cybersecurity responsibilities and duties that remain valid after termination or change of employment.

Asset Management

Objective	Action
Identification and assessment of Comcast Cable's assets.	Inventorying of assets associated with information and information processing facilities.
	Designation of ownership of assets maintained in the inventory.
	Identification, documentation, and implementation of rules for the acceptable use of information and of assets associated with information and information processing facilities.
	Return of Comcast Cable assets when no longer required.
Appropriate protection of information.	Classification of information in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.
	Information labelling in accordance with the information classification scheme adopted by Comcast Cable.
	Procedures for handling assets in accordance with the information classification scheme adopted by Comcast Cable.
Limitation of unauthorized disclosure, modification, removal, or destruction of information stored on media.	Procedures for the management of removable media in accordance with the classification scheme adopted by Comcast Cable.
	Disposal of Media when no longer required.
	Protection of media containing information are protected against unauthorized access, misuse, or corruption during transportation.

Access Control

Objective	Action
To limit access to information and information processing facilities.	Access control based on business and cybersecurity requirements.
	Provision of access consistent with authorization.
To limit access to authorized users.	Assignment of access rights via formal user registration and de-registration.
	Assignment and revocation of access rights via formal user access provisioning.
	Restriction and control of allocation and use of privileged access rights.
	Formal management processes regarding allocation of secret authentication information.
	Regular review of user access rights to assets.
To inform users about safeguarding their authentication information.	Training users regarding Comcast Cable's practices for use of secret authentication information.
To limit unauthorized access to systems and applications.	Restriction of access to information and application system functions in accordance with Comcast Cable's access control policy.
	Control of access to systems and applications by a secure log-on procedure where appropriate.
	Interactivity of password management systems and quality of passwords.
	Access to program source code.

Cryptography

Objective	Action
To effectively use cryptography to protect the confidentiality, authenticity, and/or integrity of information.	Use of cryptographic controls for protection of information.
	Use, protection, and lifetime of cryptographic keys.

Communications Security

Objective	Action
To protect information in networks and its supporting information processing facilities.	Management of networks to protect information in systems and applications.
	Segregation of information services, users, and information systems.
To secure teleworking and use of mobile devices.	Security measures to manage risks introduced by using mobile devices.
	Security measures to protect information accessed, processed, or stored at teleworking sites.
To secure information transferred within Comcast Cable and with external entities.	Protection of information during transfer .
	Contractual standards regarding the secure transfer of business information between Comcast Cable and external parties.
	Protection of information involved in electronic messaging.
	Contractual standards reflecting Comcast Cable's needs for the protection of information.

Physical & Environmental Security

Objective	Action
To limit unauthorized physical access, damage, and interference to Comcast Cable's information and information- processing facilities.	Definition of security perimeters to protect areas that contain sensitive or critical information.
	Utilization of appropriate entry controls to protect secure areas.
	Physical security for offices, rooms, and facilities.
	Physical protection against natural disasters, malicious attack, or accidents.
	Procedures for working in secure areas.
	Control and isolation of access points such as delivery and loading areas, and other points where unauthorized persons could enter the premises.
To limit loss, damage, theft, or compromise of assets and interruption to Comcast Cable's operations.	Siting of equipment to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	Protection of equipment from power failures and other disruptions caused by failures in supporting utilities.
	Protection of power and telecommunications cabling carrying data or supporting information services from interception, interference, or damage.
	Maintenance of equipment to facilitate availability and integrity.
	Appropriate security regarding off-site assets.
	Removal of sensitive data and licensed software prior to disposal or re-use.
	Appropriate protection of unattended equipment.
	Clearing desks of papers and removable storage media and clearing screens for information processing facilities.

Operations Security

Objective	Action
To facilitate correct and secure operations of information-processing facilities.	Documentation and availability of operating procedures.
	Control of changes to Comcast Cable's organization, business processes, information-processing facilities, and systems that affect cybersecurity.
	Monitoring, tuning, and capacity planning for the use of resources.
	Separation of development, testing, and operational environments.
To facilitate that information and information processing facilities are protected against malware.	Detection of, prevention of, and recovery from malware.
To protect against loss of data.	Backups of information, software, and system images.
To record events and generate evidence.	Production, maintenance, and review of logs recording user activities, exceptions, faults, and cybersecurity events.
	Protection of logging facilities and log information.
	Logging and review of system administrator and system operator activities.
	Synchronization of clocks of relevant information processing systems.
To facilitate the integrity of operational systems.	Installation and configuration of software on operational systems.
To prevent exploitation of technical vulnerabilities.	Review of information about technical vulnerabilities of information systems.
	Installation of software by users.
To minimize the impact of audit activities on operational systems.	Careful planning of audit requirements and activities.

System Acquisition, Development & Maintenance

Objective	Action
To promote cybersecurity as an integral part of information systems across the entire lifecycle.	Inclusion of cybersecurity in the requirements for new information systems or enhancements to existing information systems.
	Protection of information involved in application services passing over public networks.
	Protection of information involved in application service transactions.
To promote that cybersecurity is designed and implemented within the development lifecycle of information systems.	Rules for the development of software and systems.
	Changes to systems within the development lifecycle.
	Review and testing of business critical applications when operating platforms are changed.
	Limitation and control of modifications to software packages.
	Principles for engineering secure systems.
	Supervision and monitoring of outsourced system development.
	Testing of security functionality during development.
	Acceptance testing programs and related criteria for new information systems, upgrades, and new versions.
To promote the protection of data used for testing.	Selection, protection, and control of test data.

Supplier Relationships

Objective	Action
To promote protection of Comcast Cable's assets that are accessible by suppliers.	Documentation of cybersecurity requirements.
	Contractual requirement regarding cybersecurity risks associated with information and communications technology services and product supply chain.
To maintain an agreed level of cybersecurity and service delivery in line with supplier agreements.	Monitoring, reviewing, and auditing of supplier service delivery.
	Management of changes to the provision of services by suppliers, including maintaining and improving existing cybersecurity policies, procedures, and controls, taking into account the criticality of business information, systems, and processes involved and re-assessment of risks.

Incident Management

Objective	Action
To promote a consistent and effective approach to the management of cybersecurity incidents, including communication on security events and weaknesses.	Reporting of cybersecurity events.
	Notation and reporting of observed or suspected cybersecurity weaknesses in systems or services.
	Assessment and classification of cybersecurity events.
	Responses to cybersecurity incidents.
	Use of knowledge gained from analyzing and resolving cybersecurity incidents to reduce the likelihood or impact of future incidents.
	Identification, collection, acquisition, and preservation of information regarding cybersecurity incidents.

Business Continuity Management

Objective	Action
Embed Cybersecurity continuity in Comcast Cable's business continuity management systems.	Requirements for cybersecurity and the continuity of cybersecurity management in adverse situations.
	Periodic verification of cybersecurity continuity controls.
To promote availability of information processing facilities.	Redundancy of information processing facilities.

Compliance Management

Objective	Action
To limit breaches of legal, statutory, regulatory, or contractual obligations related to cybersecurity and of any security requirements.	Identification and documentation of relevant legislative statutory, regulatory, contractual requirements,.
	Protection of information from loss, destruction, falsification, unauthorized access, and unauthorized release.
	Use of cryptographic controls.
To promote that cybersecurity is implemented and operated in accordance with Comcast Cable's cybersecurity policies and standards.	Review and implementation of the approach to managing cybersecurity.

COMCAST