Comcast[1] Cybersecurity

Information Security Program Summary

Updated: February 2025

[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 Program provides a summary of our information security practices 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 Program is current at the time of issue and is reviewed annually.

Security Commitment

At Comcast, risk management, including the safeguarding of customer information, is a priority. 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-DSS and ISO 27001. 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 so they understand their responsibilities with respect to the protection of customer information, security of our systems and preventing breaches

Comcast has developed policies, standards, procedures and 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
Establishing 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.
	Establishing and maintenance of communication with relevant authorities.
	Establishing and maintenance of communication with special interest groups and 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 proportionality to the risk posed by the role.
	Inclusion of contractual responsibilities for cybersecurity in agreements.
Awareness of cybersecurity responsibilities	Requirements in applying cybersecurity to products, services and processes 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 labeling in accordance with the information classification scheme adopted by Comcast Cable.
	Procedures for handling assets in accordance with the information handling 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 information classification and handling scheme adopted by Comcast Cable.
	Disposal of media when no longer required.
	Protection of media containing confidential information to protect against unauthorized access, misuse, or corruption during transportation.

Access Control

Objective	Action
Limiting access to information and information-processing facilities	Access control based on business and cybersecurity requirements.
	Provision of access consistent with role requirements and authorization.
Limiting 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.
Informing users on safeguarding their authentication information	Training users regarding Comcast Cable's practices for use of secret authentication information.
Limiting unauthorized access to systems and applications	Restricting access to information and application and system functions in accordance with Comcast Cable's access control policy.
	Controlling access to systems and applications by a secure log-on procedure, such as multi-factor authentication (MFA), where appropriate.
	Interactivity of password management systems and quality of passwords.
	Accessing program source code.

Cryptography

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

Communications Security

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

Physical & Environmental Security

Objective	Action
Limiting unauthorized physical access, damage, and interference to Comcast Cable's information and information-processing facilities.	Defining security perimeters to protect areas that contain sensitive or critical information.
	Using 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.
Limiting loss, damage, theft or compromise of assets and interruption to Comcast's operations	Securing equipment to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	Protecting equipment from power failures and other disruptions caused by failures in supporting utilities.
	Protecting power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.
	Maintaining equipment to facilitate availability and integrity.
	Appropriate securing of off-site assets.
	Removing sensitive data and licensed software from hardware prior to disposal or re-use.
	Appropriately protecting unattended equipment.
	Clearing desks of papers and removable storage media and clearing screens for information-processing facilities.

Operations Security

Objective	Action
Facilitating correct and secure operations of information-processing facilities	Documentation and availability of operating procedures.
	Controlling changes to Comcast's organization, business processes, information-processing facilities, and systems that impact cybersecurity.
	Monitoring, tuning, and capacity-planning for the use of resources.
	Separation of development, testing, and operational environments.
Ensuring that information and information-processing facilities are protected against malware	Detecting, preventing, and recovering from malware.
Protecting against loss of data	Backing up information, software, and system images.
Recording events and generating evidence	Producing, maintaining, and reviewing logs, and record-keeping user activities, exceptions, faults and cybersecurity events.
	Protecting logging facilities and logging information.
	Logging and reviewing system administrator and system operator activities.
	Synchronization of clocks for relevant information-processing systems.
Facilitating the integrity of operational systems	Installing and configuring software on operational systems.
Preventing exploitation of technical vulnerabilities	Reviewing information about technical vulnerabilities of information systems.
	Analyzing software installed by users.
Minimizing the impact of audit activities on operational systems	Careful planning of audit requirements and activities.

System Acquisition, Development & Maintenance

Objective	Action
Promoting cybersecurity as an integral part of information systems across the entire lifecycle	Including cybersecurity in the requirements for new information systems and enhancing existing information systems.
	Protection of information involved in application services passing over public networks.
	Protecting information involved in application service transactions.
Promoting the design and implementation of cybersecurity throughout the development lifecycle	Imposing rules for the development of software and systems.
	Adapting systems within the development lifecycle.
	Reviewing and testing business-critical applications when operating platforms are changed.
	Limiting and controlling modifications to software packages.
	Observing principles for engineering secure systems.
	Supervising and monitoring outsourced system development.
	Testing security functionality during development.
	Acceptance testing programs and related criteria for new information systems, upgrades, and new versions.
Promote the protection of data used for testing	Selecting, protecting, and controlling test data.

Supplier Relationships

Objective	Action
Promoting the protection of Comcast's assets that are accessible by suppliers	Documenting cybersecurity requirements.
	Imposing contractual requirements regarding cybersecurity risks associated with information and communications technology services and product supply chain.
Maintaining an agreed-upon level of cybersecurity and service delivery in line with supplier agreements.	Monitoring, reviewing, assessing and auditing supplier service delivery.
	Managing changes to the provision of services by suppliers, including maintaining and improving existing cybersecurity policies, procedures, and controls, and addressing the criticality of business information, systems and processes involved and re-assessment of risks.

Incident Management

Objective	Action
Promoting a consistent and effective approach to the management of cybersecurity incidents, including communication on security events and gaps	Reporting cybersecurity events.
	Notating and reporting observed or suspected cybersecurity weaknesses in systems or services.
	Assessing and classifying cybersecurity events.
	Responding to cybersecurity incidents.
	Reviewing knowledge gained from analyzing and resolving cybersecurity incidents to reduce the likelihood or impact of future incidents.
	Identifying, collecting, acquiring and preserving information relating to cybersecurity incidents.

Business Continuity Management

Objective	Action
Embedding cybersecurity continuity in Comcast's business continuity management systems	Imposing requirements for cybersecurity and the continuity of cybersecurity management in adverse situations.
	Periodically verifying cybersecurity continuity controls.
Promoting the availability of information-processing facilities	Managing the redundancy of information-processing facilities.

Compliance Management

Objective	Action
Minimizing gaps in legal, statutory, regulatory, and contractual obligations related to cybersecurity	Identifying and documenting relevant legislative, statutory, regulatory, and contractual requirements.
	Protecting information from loss, destruction, falsification, unauthorized access and unauthorized release.
	Using cryptographic controls.
Promoting implementation and operation of cybersecurity controls in accordance with Comcast's policies and standards	Effectively reviewing and managing cybersecurity controls.

COMCAST