Cybersecurity Policies & Standards Reference

For Public Dissemination

Maxar is dedicated to protecting our network and systems from cyberthreats and the loss of customer, team member and corporate information. Maxar is committed to continuous improvement and maturation in our customer information systems and network security capabilities. We aim to secure Maxar's environment against evolving threats while protecting our critical business functions, brand and reputation. Employees are responsible for participating in security awareness training and initiatives. Further, Maxar expects suppliers to implement practices and procedures to ensure the security of their supply chain. Third-party risk is assessed prior to a supplier processing, storing or transmitting Maxar information.

This document is approved in accordance with the Maxar Policy Governance program.
Records of the: review, approval and version history of this document are retained in PolicyTech.

Cybersecurity Policies

Audience: Content is relevant to all Maxar team members.

Policies	Purpose
Acceptable Use Policy (AUP)	Establishes the obligations, restrictions, and acceptable use of Maxar Information Technology (IT) systems, assets, data, and network resources in order that these systems are protected.
Information Security Policy	Establishes requirements for the management implementation of cybersecurity controls to protect the confidentiality, integrity, and availability of information systems and assets on Maxar's network in compliance with NIST 800-171 and CMMC 2.0.

Cybersecurity Standards

Audience: The Cybersecurity standards require adherence from **all IT system owners, administrators and/or users who are designing, implementing and/or administering systems**. Operationalizing these standards is required to implement the foundational security controls needed for compliance as well as to safeguard Maxar and Maxar customer information. Additionally, these standards are being shared Maxar-wide for general awareness and understanding because they impact the user experience.

Standards	Description
Access Control Standard	Defines rules to control access to data and systems to protect against improper or unauthorized access. Includes account management, privileged accounts, access enforcement, remote and wireless access, mobile devices, and externally/publicly accessible systems.
Awareness and Training Standard	Defines requirements for a formal training and education program to inform Maxar team members about cyber threats and preventive actions, risks, and indicators of insider threat. Establishes the requirement for all Maxar personnel to complete assigned mandatory annual cybersecurity awareness training and to acknowledge the AUP annually.
Audit and Accountability Standard	Defines requirements for the creation, protection, retention, and review of Maxar information system audit logs and records to identify and manage potential risks from event logging and transaction monitoring. Includes audit information and logging and time stamps.
Configuration Management Standard	Defines configuration management requirements that apply to Maxar information systems and cloud environments to include servers, network devices, workstations, systems/network design, and hardware and software to maintain asset inventory and baseline configuration settings. Includes change control and restriction of nonessential capabilities.
Identification and Authentication Standard	Defines requirements for the secure identification and authentication of users into Maxar's information systems and assets. Includes governing user passwords, multi-factor -authentication (MFA) and other credentials.
Incident Response Standard	Defines operational and test incident handling capabilities to support risk mitigation activities that include preparation, detection, analysis, containment, recovery, and response activities to cyber incidents. This standard also outlines requirements for tracking, documenting, and reporting potential cybersecurity incidents.
Maintenance Standard	Defines requirements for safeguarding activities during routine system maintenance and repair of Maxar information systems that are onsite, taken offsite, and serviced by Maxar or non-Maxar personnel.

Media Protection Standard	Defines requirements for the protection, sanitization, and disposal of digital and non-digital media and the data stored within. Includes removable media, media containing Controlled Unclassified Information (CUI), marking, and transport.
Personnel Security Standard	Defines requirements for mitigating risks from personnel threats through the deployment of personnel screening procedures, access agreements, and management of position terminations and transfers. This standard does not pertain to the processing or handling of security clearances.
Physical Protection Standard	Defines requirements and safeguards for the management of physical security and environmental controls for areas used to house Maxar information systems equipment and data. Includes visitor control and alternate work sites.
Risk Assessment Standard	Defines requirements for incorporating consistent and effective risk assessment into organizational planning processes. The intent is to manage the impact of potential risks and vulnerabilities. Includes information about vulnerability scanning and remediation timelines.
Security Assessment Standard	Defines requirements for identifying and managing risks across the Maxar environment through the documentation, assessment, monitoring and subsequent remediation actions of security controls. This standard enforces continuous monitoring of system compliance to the specified set of security requirements as documented in a System Security Plan (SSP).
System and Communications Protection Standard	Defines requirements to identify, monitor, and control all systems and system communications, including those that store or transmit CUI. Enables Maxar to protect, control, and monitor systems against the loss or exposure of Maxar data. Includes boundary protection, cryptography, communication sessions, and protection of data at rest.
System and Information Integrity Standard	Defines requirements for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes and inadequate error handling. Provides guidance for the implementation of system configuration, security, and error handling best practices. Includes vulnerability remediation timelines.