SmartSuite

Framework / Cybersecurity / Other

# China MLPS v2.0 – Levels 1–5

China MLPS 2.0 requires organizations to classify and protect information systems based on importance to national security and public interests.

## What it is

China MLPS 2.0 — Multi-Level Protection Scheme (Classified Protection of Cybersecurity) is a regulatory framework that enables organizations to classify and protect information systems based on their importance to national security, economic stability, and public interests. The scheme establishes requirements for implementing cybersecurity controls and risk management practices that correspond to different levels of system criticality.

Issued by the Ministry of Public Security (MPS) of China, MLPS 2.0 applies to both public and private sector organizations operating or managing information systems within China. The regulation covers areas such as data protection, risk assessment, network security, access controls, and incident response, with a tiered approach to strengthening compliance oversight and cybersecurity resilience.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>National Cybersecurity Center of China | TYPE<br>Framework | VERSION<br>MLPS 2.0 — Multi-Level Protection Scheme |
| EFFECTIVE<br>2019 | DOMAIN<br>Cybersecurity | FAMILY<br>Other |
| REGION<br>China | ADOPTION MODEL<br>Regulatory Compliance | IMPLEMENTATION COMPLEXITY<br>Very High |

Source: https://www.ncsc.gov.cn/

## Why it matters

- **Strengthen cybersecurity governance** Establishes a formal structure for identifying, classifying, and protecting information systems according to risk and criticality.
- **Enhance regulatory alignment** Supports compliance with China's national cybersecurity requirements, helping organizations meet evolving legal and policy obligations.
- **Protect sensitive data assets** Implements graduated security controls to safeguard critical data, reducing the likelihood of breaches or unauthorized disclosures.
- **Increase audit readiness** Provides a documented trail of risk assessments, controls, and procedures to facilitate regulatory inspections and third-party audits.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

## How SmartSuite supports MLPS 2.0

### System Classification and Protection Levels

Classify systems into MLPS levels (Level 1–5) and track required protection measures.

### Control Framework by Security Level

Structure technical and organizational controls aligned to MLPS level requirements.

### System Risk Assessment and Gap Remediation

Assess system risks, identify control gaps, and prioritize remediation activities.

### Identity, Authentication, and Network Protection

Manage identity, authentication, and network protection controls across systems.

### Monitoring, Logging, and Incident Response

Track system activity, detect anomalies, and manage incident response workflows.

### MLPS Compliance Tracking and Certification Readiness

Provide dashboards showing control coverage, system classification status, and MLPS compliance readiness.

## Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5

## Official resources

### MLPS 2.0 Official Guidelines

Provides the official guidelines for implementing the Multi-Level Protection Scheme in China.

ncsc.gov.cn

### MLPS 2.0 Technical Requirements

Outlines technical requirements necessary for compliance with the MLPS framework.

ncsc.gov.cn

### MLPS 2.0 Implementation Guide

Describes strategies for organizations to effectively implement MLPS 2.0 standards.

ncsc.gov.cn

### MLPS 2.0 Compliance Framework

Defines the compliance framework for ensuring adherence to national cybersecurity requirements.

ncsc.gov.cn

## Frequently asked questions

### What is China MLPS 2.0 used for?

China MLPS 2.0 is used to classify and secure information systems according to their significance to national security, economic activities, and public interests. It sets forth cybersecurity requirements and controls tailored to different protection levels, driving risk-based security management in organizations operating in China.

### Is compliance with China MLPS 2.0 mandatory?

Yes, compliance with MLPS 2.0 is mandatory for all organizations, both domestic and foreign, that operate or manage information systems within China. Non-compliance can result in regulatory penalties, operational restrictions, or other legal consequences.

### What types of organizations and systems are covered by China MLPS 2.0?

MLPS 2.0 applies to all public and private sector organizations using information systems in China, including critical infrastructure, cloud service providers, and enterprises handling sensitive data. The framework covers IT, OT, and networked systems used for national, economic, or social functions.

### How are information systems classified under MLPS 2.0?

Information systems are classified into five ascending protection levels based on their potential impact on national security, social stability, economic development, or public interests in the event of a security breach. Each level prescribes progressively stricter security and compliance requirements.


Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### What are the main compliance artifacts or deliverables under MLPS 2.0?

Key compliance artifacts include classification assessment reports, gap analyses, security policies, control implementation evidence, risk registers, and documentation of regular security assessments and remediation actions. These documents are reviewed during regulatory audits.

### How does MLPS 2.0 compare to international cybersecurity frameworks?

MLPS 2.0 is distinct in its tiered approach and mandatory national application, but shares concepts like risk management, access controls, and auditability with frameworks such as ISO 27001 or NIST CSF. However, it specifically aligns with China's cybersecurity regulations and legal requirements.

### What are the ongoing compliance requirements for China MLPS 2.0?

Continuous compliance requires periodic risk assessments, regular security testing, incident response planning, documentation updates, and ongoing monitoring of controls. Organizations must be prepared for regulatory inspections and demonstrate remediation of any findings.

### How would SmartSuite support China MLPS 2.0?

SmartSuite streamlines MLPS 2.0 compliance by enabling centralized management of control implementation, risk tracking, and policy documentation according to each protection level. The platform facilitates evidence collection for audits, tracks remediation activities, and offers dashboards for ongoing compliance monitoring and reporting, supporting audit readiness and regulatory engagement.

License included / downloadable: Yes MLPS guidance is published by Chinese government authorities and is publicly available through official regulatory sources.

Full framework page and mappings: smartsuite.com/frameworks/china-mlps-2-0-multi-level-protection-scheme