safous

JAMA/JAPIA CYBERSECURITY CHECKLIST

Meet JAMA/JAPIA Cybersecurity Guidelines Requirements With Safous

The JAMA/JAPIA Cybersecurity Guidelines (Ver. 2.3) provide a common baseline for protecting confidential information, design data, production systems, and both IT and OT environments across the Japanese automotive supply chain.

Developed by the Japan Automobile Manufacturers Association (JAMA) and the Japan Auto Parts Industries Association (JAPIA), these guidelines define essential controls for governance, supplier management, access control, secure connectivity, authentication, monitoring, and incident response.

Safous helps Automotive OEMs and Tier 1 and Tier 2 suppliers address parts of the guidelines with Zero Trust remote access and identity-based access governance. Whether managing supplier maintenance or internal access policies, Safous provides the security features to support alignment with JAMA/JAPIA's guidelines – without expanding the attack surface.

Disclaimer: This checklist illustrates how Safous technically supports selected controls of the JAMA/JAPIA Cybersecurity Guidelines Ver. 2.3. Organizational governance, internal policies, training, and contractual processes must be addressed separately by each company.

Safous and JAMA/JAPIA Cybersecurity Guidelines Ver. 2.3

JAMA/JAPIA Label	Regulation	How Safous Helps
Labels 5-6 – System & procedures in adverse situations	18-24 – Define systems and procedures for incident response and recovery	Supports rapid incident containment with instant session termination, account disabling, and full session replay for root-cause analysis and reporting.
Label 8 – Information security requirements between companies	41-48 – Manage supplier security, confidential information handling, and contract-lifecycle access control	Provides secure, identity-based vendor and supplier access with MFA, time-bound approvals, and full session recording; can revoke access instantly at contract end to strengthen accountability.
Label 9 – Access rights	49-53 – Define, grant, review, and revoke system access rights; maintain secure audit logs	Enforces least-privilege access with RBAC, JIT elevation, and supervised sessions. All user actions are fully logged and recorded to support compliance and audit readiness.
Label 10 – Management of information assets (information)	54-58 – Classify confidential information and implement classification-aligned controls	Applies strict controls (MFA, session recording, approvals) when users access high-confidentiality systems such as design, quality, or production platforms.
Label 11 – Management of information assets (equipment/devices)	59-65 – Maintain IT/OT asset inventories and enforce appropriate usage rules and access pathways	Provides asset-level, not network-level, access to minimize exposure and secure connections to OT/IT assets; detailed logs support asset governance and lifecycle review.
Label 12 – Risk response	66-69 – Identify cybersecurity risks and plan/implement mitigation measures	Uncovers risks related to remote access, privileged operations, and supplier access. Logs and recordings support risk assessments and help prioritize corrective actions.

JAMA/JAPIA Label	Regulation	How Safous Helps
Label 14 – Understanding the statuses of external connections	74-78 – Document and monitor external and cloud connections across the organization	Consolidates external access into one secure gateway, providing visibility into who connects to which systems and enabling accurate network and data-flow mapping.
Label 15 – In-house connection rules	79-83 – Establish rules for internal network usage, remote access, and BYOD	Enforces Zero Trust app-level access to prevent unmanaged devices from joining internal networks; remote work rules can be implemented consistently across roles and locations.
Label 17 – Communication control	103-112 – Control network communication, filtering, segmentation, and encryption	Operates as a Zero Trust proxy with fully encrypted sessions. WAAP/WAF-style protection reduces the number of exposed services and improves boundary defense and segmentation.
Label 18 – Authentication & approval	113-122 – Enforce unique IDs, MFA, strong passwords, approval workflows, and authentication monitoring	Integrates with enterprise IdPs to enforce MFA, SSO, step-up authentication, and approval-based privileged access; identity-bound logs support verification and audit assurance.
Label 19 – Applying patches and updates	123-128 – Ensure proper patching and vulnerability remediation	Supports secure execution, logging, and auditability of patching and maintenance activities.
Label 20 – Data protection	129-130 – Encrypt and protect data in motion and verify external files	Encrypts all remote communication and proxy applications without copying data; browser isolation protects privileged users from malicious external content.
Label 23 – Detecting unauthorized access	142-147 – Monitor, detect, and block unauthorized access; collect logs for investigation	Provides identity-linked telemetry, session replay, abnormal login detection, and SIEM/SOC integration to help detect intrusions and support forensics.

Simplify JAMA/JAPIA Cybersecurity Alignment With Safous

Safous centralizes and secures remote access to help organizations that manage third-party or maintenance access in IT/OT environments align with parts of the JAMA/JAPIA Guidelines Ver. 2.3 – all while reducing operational risk.

Talk to our team today to learn more about how Safous supports secure vendor access, Zero Trust remote operations, and automotive supply chain security.

EXPLORE SAFOUS