Here’s the complete **Logging & Monitoring Policy** in plain text (no formatting requirements, copy-paste ready for Word).

Logging & Monitoring Policy

1. Purpose
The purpose of this policy is to establish Toyota’s enterprise-wide approach to logging and monitoring of information systems. Effective log collection, monitoring, and analysis are essential to:
* Detect and respond to cybersecurity threats in a timely manner,
* Ensure accountability and traceability of user and system actions,
* Support regulatory and legal obligations,
* Provide forensic evidence in the event of incidents, audits, or litigation, and
* Strengthen Toyota’s overall resilience against cyber risk.

This policy aligns with Toyota’s commitment to safeguarding critical business processes, protecting customer trust, and ensuring compliance with industry standards and regulations, including NIST Cybersecurity Framework (CSF) 2.0, ISO 27001, PCI DSS, SOX, and FFIEC guidance.

1. Scope
This policy applies to all Toyota entities, subsidiaries, business units, employees, contractors, and third-party service providers that design, operate, or manage information systems processing Toyota’s data.
* Systems in Scope: All production systems, business-critical non-production systems, corporate networks, applications, databases, and cloud services (IaaS, PaaS, SaaS).
* Data in Scope: All categories of data classified as Toyota Confidential, Toyota Restricted, or subject to legal/regulatory protection (e.g., personally identifiable information, payment card data, financial records, intellectual property).
* Users in Scope: All employees, contractors, and service providers with access to Toyota systems.
1. Policy Principles
Toyota’s logging and monitoring program is guided by the following principles, which reflect the organization’s philosophy for managing cyber risk and compliance:
2. Proactive Detection over Reactive Response – Toyota emphasizes early threat identification through continuous monitoring and advanced analytics, enabling proactive defense rather than delayed response.
3. Forensic Readiness – Logs are captured in standardized formats, synchronized with authoritative time sources, and stored in tamper-resistant repositories to ensure reliability during investigations and audits.
4. Accountability and Traceability – All significant user and system activities must be attributable, ensuring Toyota can hold individuals and services accountable for their actions.
5. Least Privilege Access to Logs – Access to log data is restricted on a need-to-know basis, applying role-based controls to reduce the risk of unauthorized disclosure.
6. Integrity and Non-Repudiation – Logs must remain unaltered once recorded, with protections in place to prevent deletion or manipulation.
7. Holistic Visibility – Logging and monitoring must cover the enterprise end-to-end: networks, applications, endpoints, cloud platforms, and third-party integrations. Centralized monitoring eliminates blind spots.
8. Risk-Based Monitoring – Critical and sensitive systems are prioritized for enhanced logging and monitoring based on Toyota’s cyber risk appetite, threat intelligence, and regulatory exposure.
9. Continuous Improvement and Adaptability – The logging and monitoring program evolves in line with new threats, leveraging lessons learned, red team exercises, and industry intelligence to maintain effectiveness.
10. Regulatory Alignment with Toyota Standards – Practices are aligned to global frameworks (NIST CSF 2.0, ISO 27001, PCI DSS, SOX, FFIEC), ensuring audit readiness and demonstrating Toyota’s commitment to compliance.
11. Shared Responsibility with Third Parties – Vendors and service providers impacting Toyota’s operations must implement equivalent logging and monitoring controls or provide Toyota with sufficient visibility into their environments.
12. Policy Statements
13. Comprehensive Logging Requirement
All Toyota systems, applications, databases, and network components must generate and retain logs that capture security-relevant events. Logs must include sufficient detail (timestamps, user identity, source/destination, event type, and outcome) to support investigations, audits, and accountability.
14. Centralized Collection and Analysis
All security logs must be forwarded to Toyota’s centralized Security Information and Event Management (SIEM) system or equivalent monitoring platform. Centralization ensures enterprise-wide visibility, event correlation, and a single authoritative repository for compliance evidence.
15. Active Monitoring and Threat Detection
Security logs must be actively monitored on a continuous basis. Automated detection rules, correlation engines, and threat intelligence integrations must be used alongside human analysis to identify suspicious or malicious activity. Detection rules must be regularly tuned to reduce false positives and adapt to emerging threats.
16. Incident Response Integration
All detected events that indicate potential compromise, misuse, or non-compliance must be investigated and escalated in accordance with Toyota’s Incident Response Plan (IRP). Escalation timelines must reflect event severity, with high-priority alerts requiring immediate attention.
17. Retention and Protection of Logs
Logs must be retained for at least 12 months, with the most recent 90 days readily available for investigation. Logs must be encrypted at rest and in transit, stored in secure repositories, and protected from tampering through integrity controls. Longer retention periods must be applied where required by regulation or business need.
18. Time Synchronization
All log sources must synchronize with Toyota’s approved authoritative time source (e.g., NTP servers). Accurate time synchronization is essential for correlating logs across distributed environments and reconstructing attack timelines.
19. Roles and Accountability
Logging and monitoring responsibilities must be clearly assigned. System Owners are responsible for ensuring logging is enabled; the SOC is responsible for daily monitoring and alert triage; IT Operations is responsible for maintaining infrastructure; the Cyber Risk Assurance Lead is accountable for overall governance, oversight, and compliance reporting.
20. Continuous Program Improvement
Logging and monitoring capabilities must be periodically tested, reviewed, and improved. This includes quarterly SIEM rule tuning, annual red team/purple team exercises, and regular integration of new log sources and detection rules based on lessons learned and threat intelligence.
21. Third-Party Logging and Monitoring
All third-party service providers must comply with Toyota’s logging and monitoring requirements. Where integration into Toyota’s SIEM is not feasible, providers must deliver log exports, monitoring dashboards, or attestations demonstrating equivalent controls.

Would you like me to now expand the **Standards section** in the same style (detailed “control objectives” form) so it aligns seamlessly with this polished policy?