HONDA

2025 Security Policy

Office of Information Technology
Security Department

Greensburg, Indiana
June 6, 2025

Table of Contents

Glossary

Access Control Mechanisms that limit access to systems, networks, or data based on user identity and permissions.

ACL (Access Control List) A list of permissions attached to an object specifying which users or systems can access it and what operations they can perform.

AI (Artificial Intelligence) Technology that simulates human intelligence processes, such as learning and problem-solving, often used in threat detection.

Antivirus Software designed to detect, prevent, and remove malicious software (malware).

Asset Any item of value to the organization, including data, hardware, software, and personnel.

Authentication The process of verifying a user's identity before allowing access.

Authorization The process of granting or denying specific permissions to a user or system after authentication.

Availability One of the CIA triad components; ensures that information and systems are accessible when needed.

Backup A copy of data stored separately to enable recovery in case of data loss or corruption.

Biometric Authentication Authentication method using unique biological traits such as fingerprints or facial recognition.

BYOD (Bring Your Own Device) A policy allowing employees to use their personal devices for work purposes.

CIA Triad The core principles of security: Confidentiality, Integrity, and Availability.

Confidentiality Ensuring that information is only accessible to those with authorized access.

Cybersecurity Practices and technologies used to protect systems, networks, and data from cyber threats.

Cybersecurity and Infrastructure Security Agency (CISA) A U.S. federal agency responsible for protecting critical infrastructure from cyber threats

Data Classification The process of categorizing data based on sensitivity (such as public, internal, restricted, confidential).

Data Encryption The process of encoding data to prevent unauthorized access, ensuring confidentiality during storage and transmission

Data Loss Prevention (DLP) Technologies that monitor and prevent the unauthorized transmission of sensitive data.

Disaster Recovery (DR) A set of policies and procedures for restoring critical systems after a catastrophic event.

DMZ (Demilitarized Zone) A network segment that acts as a buffer zone between internal systems and external networks.

Encryption The process of converting data into a coded form to prevent unauthorized access.

Endpoint Security Measures to secure devices like laptops, desktops, and mobile devices.

FDE (Full Disk Encryption) Encrypts all data on a disk drive to protect it from unauthorized access.

Firewall A network security device that monitors and filters incoming and outgoing network traffic.

Governance, Risk, and Compliance (GRC) An integrated framework for aligning IT and business objectives with regulatory compliance and risk management

GPO (Group Policy Object) A set of rules in Microsoft environments used to control the working environment of user and computer accounts.

HSM (Hardware Security Module) A physical device that safeguards and manages digital keys for strong authentication.

Incident Response (IR) The structured approach for handling and mitigating the effects of security incidents.

Integrity Ensures that data is accurate and has not been tampered with.

IPS (Intrusion Prevention System) A system that monitors network traffic and takes actions to prevent detected threats.

Least Privilege A principle that users should only have the minimum level of access necessary to perform their job.

Logging Recording events and actions on a system for monitoring and auditing.

Malware Malicious software, such as viruses, worms, trojans, or ransomware.

MFA (Multi-Factor Authentication) A security mechanism requiring two or more authentication methods.

Password Policy Rules governing password creation, complexity, reuse, and expiration to improve security.

Patch Management The process of distributing and applying updates to software.

Phishing A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity.

PKI (Public Key Infrastructure) A framework for managing digital certificates and public-key encryption.

Policy Exception A formally approved deviation from standard policy due to a specific business need.

Ransomware Malware that encrypts a user's data and demands payment for the decryption key.

Recovery Time Objective (RTO) The maximum acceptable time to restore a business process after a disruption

Remote Access The ability to access a system or network from a remote location, often through VPN.

Risk Assessment The process of identifying and evaluating potential risks to organizational assets.

Role-Based Access Control (RBAC) Access control method based on users' roles within the organization.

SED (Self-Encrypting Drive) A drive that automatically encrypts and decrypts data on the fly using built-in hardware.

SIEM (Security Information and Event Management) A system that aggregates and analyzes security event data from across an organization.

Social Engineering Manipulating people into revealing confidential information or performing unsafe actions.

Third-Party Risk Management The process of assessing and managing risks posed by vendors or external service providers.

TPM (Trusted Platform Module) A hardware chip that provides secure cryptographic functions, commonly used for device encryption.

VPN (Virtual Private Network) A secure communication channel over the internet.

Vulnerability A weakness in a system that could be exploited to compromise it.

Zero Trust Architecture A security model that assumes no implicit trust; verifies every request as though it originated from an open network.

Chapter 1

Governance, Risk, and Compliance

1.1 Purpose

The purpose of the Governance, Risk, and Compliance (GRC) program is to establish a structured, integrated approach to managing these activities at Honda's Indiana manufacturing plant. The GRC program is designed to align the plant's business objectives with relevant legal, regulatory, and internal requirements while effectively managing risk. By coordinating governance (policies and oversight), risk management, and compliance efforts, Honda ensures that its operations remain efficient, secure, and ethically and legally sound.

1.2 Scope

The scope of Honda's GRC program covers all major operational areas of the Indiana manufacturing facility, including production processes, information systems, employee activities, and interactions with suppliers and partners. It encompasses the governance policies, risk management processes, and compliance obligations that apply to these areas. This chapter addresses GRC practices across a range of domains—from data security and privacy, quality control, and occupational safety to environmental protection and supply chain oversight. Clearly defining the scope ensures that GRC efforts remain focused on relevant areas and do not become overly broad or unmanageable.

1.3 Establishing Policy

Effective governance requires a strong foundation of policies, ethics, and leadership oversight. Honda ensures that:

- **Policies and Ethical Standards:** Honda will define formal policies that articulate the rules of conduct and ethical standards expected of all employees and partners. These policies create an accountability framework, clearly outlining acceptable behavior and practices, and they help instill a culture of integrity throughout the organization.

- **Strategic Alignment:** All GRC activities and policies are aligned with Honda's overall business objectives and long-term goals. This alignment ensures that risk management and compliance efforts support (and do not hinder) the plant's operational performance and strategic direction. GRC initiatives are evaluated in the context of how they help achieve Honda's mission and maintain its reputation.

- **Leadership Oversight:** Senior management at Honda's Indiana plant is actively involved in reviewing and guiding GRC efforts. Leadership oversight provides accountability and demonstrates top-down commitment to governance and risk awareness. A governance structure (such as a GRC committee or designated executives) oversees the implementation of policies and controls, ensuring that GRC remains a priority and that issues are addressed promptly.

- **Roles and Responsibilities:** Clear roles and responsibilities for GRC activities are established. Honda assigns specific responsibility for areas such as compliance monitoring, risk assessment, and policy enforcement to appropriate roles (a compliance officer, risk manager, IT security lead, environmental health & safety coordinator, etc.). By delineating who is accountable for each aspect of governance, risk, and compliance, the company ensures effective execution and avoids gaps or overlaps in coverage.

1.4 Risk Management

Managing risk is a continuous, proactive process at the plant, involving identification of risks, implementation of mitigations, and ongoing monitoring:

- **Risk Identification:** Honda regularly conducts risk assessments to identify potential risks that could hinder the plant's objectives. These include operational risks (such as equipment failures or production downtime), safety hazards (workplace accidents or injuries), supply chain disruptions (late deliveries, quality issues with suppliers, or single-source dependencies), financial risks (cost fluctuations, budget overruns, or market changes), and cybersecurity threats (malware infections, data breaches, or system outages).

- **Risk Mitigation Strategies:** For each significant risk identified, Honda develops and implements plans to reduce or eliminate that risk. Mitigation strategies might include engineering solutions and preventive maintenance to address operational and safety risks, establishing backup suppliers or increasing inventory for critical materials to handle supply chain risks, purchasing insurance or setting aside contingency funds for financial risks, and deploying cybersecurity measures (firewalls, antivirus, access controls, etc.) to combat digital threats. Each mitigation plan is documented and assigned to responsible owners.

- **Continuous Monitoring and Evaluation:** Risk management efforts are continuously monitored and evaluated. Honda will track key risk indicators and incident reports to gauge whether risk levels are increasing or if mitigation measures are effective. Periodic reviews of the risk register

are conducted, and the GRC team adjusts risk mitigation strategies as needed (for example, if a new risk emerges or if existing controls are not sufficient). This ongoing evaluation helps the plant adapt to changing conditions and ensures that the risk management process remains dynamic and responsive.

1.5 Data Classification

Honda will implement a data classification scheme to categorize information assets based on sensitivity and importance. By defining clear classification levels and criteria, the company can ensure that each type of data is handled with appropriate security controls and access restrictions. All data assets, both structured (such as databases, production schedules, and customer or supplier records) and unstructured (such as emails, design documents, and reports), will be inventoried and classified under this scheme.

Classification Level	**Description and Examples**
Public	Information approved for public release. Disclosure of public data poses no risk to Honda. *Examples: Press releases, publicly available company information, marketing materials.*
Internal	Non-public information intended for internal use within Honda. Typically of low sensitivity, with limited impact if disclosed outside the company. *Examples: Internal memos, routine operational reports, organizational charts and phone directories.*
Restricted	Sensitive information that should be restricted to specific groups or departments. Unauthorized disclosure could have a significant negative impact on the business or competitive position. *Examples: Supplier contracts and pricing, detailed production process documentation, non-public technical specifications, project plans.*
Confidential	Highly sensitive information with strict access controls, limited to only those who absolutely need it. Unauthorized disclosure of confidential data could cause severe financial, legal, or reputational damage. *Examples: Trade secrets, proprietary research and development data, critical product designs, personally identifiable information of employees or customers.*

Appropriate handling requirements (such as encryption, access control, or audit logging) will be specified for each classification level. The data classification policy helps employees understand how to treat information and prevents both accidental and malicious data leaks by ensuring higher-sensitivity data receives stronger protections.

1.6 Quality Management

Quality management ensures that Honda's products meet strict standards and customer expectations. The Indiana plant employs several key quality control

practices:

- **Incoming Raw Material Inspection:** All incoming raw materials and components are subject to stringent quality checks before they enter production. By inspecting materials upon arrival (for example, verifying the specifications and quality of steel, plastic parts, electronics, etc.), Honda prevents defective or substandard inputs from causing problems later in the manufacturing process.
- **In-Process Inspections:** Quality inspections are carried out at various stages of the manufacturing process. This might include checking critical dimensions, tolerances, and assembly steps on the production line at defined checkpoints. Regular in-process inspection helps identify any deviations from quality standards early, so that issues can be corrected immediately—reducing waste, rework, or potential recalls.
- **Document Control:** A robust document control system is implemented to manage all quality-related documents. This system governs the creation, review, revision, and archiving of documents such as standard operating procedures (SOPs), work instructions, quality manuals, inspection forms, and records of changes. Maintaining strict document control ensures that everyone is working off the correct, most up-to-date procedures and that there is traceability for any changes made (which is critical for both quality consistency and compliance audits).

Additionally, Honda's quality management system is aligned with recognized industry standards (such as ISO 9001 and the automotive-specific IATF 16949). By following these structured quality management frameworks, the plant strives for continuous improvement in processes and products, defect reduction, and high customer satisfaction.

1.7 Occupational Health & Safety

The health and safety of employees are top priorities in Honda's operations. The plant's Occupational Health and Safety (OHS) program includes:

- **Leadership Commitment:** Honda's leadership at the Indiana plant demonstrates strong commitment to workplace health and safety. Management establishes clear OHS policies and objectives, and allocates the necessary resources to support safety initiatives. Leaders also lead by example in following safety rules and procedures. A culture of safety is promoted from the top down, with management encouraging active worker involvement—such as through joint management-worker safety committees—so that employees participate in hazard identification, safety discussions, and program evaluations.
- **Hazard Identification and Risk Assessment:** Formal processes are in place to continually identify hazards in the workplace and assess their associated risks. This includes routine inspections and job safety analyses to spot potential dangers (machine guarding issues, exposure to hazardous chemicals or fumes, ergonomic stresses in assembly tasks, electrical hazards, and common issues like slips or trips). For each identified hazard,

a risk assessment is performed considering the likelihood of an incident and the potential severity of injuries or illnesses. Based on this assessment, Honda implements risk mitigation measures—ranging from engineering controls (such as installing safety guards and ventilation systems) to administrative controls (safety procedures, work rotation to reduce repetitive stress), and providing appropriate personal protective equipment (PPE)—with the aim of eliminating the hazard or minimizing the risk.

- **Compliance with Regulations and Standards:** The plant complies with all applicable occupational safety and health regulations. This includes adherence to OSHA standards (enforced in Indiana via the Indiana Occupational Safety and Health Administration, IOSHA) covering hazard communication (ensuring employees know about chemical hazards), emergency action and fire prevention plans, machine safeguarding and lockout/tagout procedures for equipment maintenance, use of PPE, fall protection requirements, and more. Honda also looks to industry best practices and standards for guidance; for example, the company may implement an occupational health and safety management system in line with ISO 45001 to provide a structured framework for managing OHS risks. Any other relevant national or international safety guidelines applicable to the manufacturing environment are identified and followed.

- **Safety Programs and Training:** Comprehensive safety programs and training ensure that employees are well-informed and prepared to work safely. All employees receive training on general workplace safety and on specific job hazards before starting work, and refresher trainings are conducted at regular intervals. Training covers proper operation of machinery and tools, safe handling of hazardous materials, emergency response procedures (such as what to do in case of a fire or chemical spill), and correct use of PPE for tasks that require it. By investing in ongoing education and drills, Honda ensures that safety procedures are understood, remembered, and practiced consistently on the factory floor.

- **Incident Management and Continuous Improvement:** Honda has clear procedures for incident reporting and investigation. Employees are encouraged and required to report any workplace incidents, accidents, or near-misses immediately. Each report is investigated to determine root causes, and corrective actions are implemented to prevent similar incidents in the future. The plant tracks safety performance indicators (like injury frequency rates, near-miss counts, audit findings) and regularly reviews the effectiveness of its OHS programs. Management conducts periodic safety meetings and program reviews, using these insights to drive continual improvement. Through this proactive incident management and feedback process, Honda aims to continuously improve its OHS performance and move toward the goal of zero workplace injuries or illnesses.

1.8 Environmental Management

Honda is committed to environmental responsibility and compliance in its manufacturing operations. The plant's environmental management program focuses on:

- **Environmental Compliance:** The facility will comply with all applicable U.S. federal and Indiana state environmental laws and regulations. Key requirements include the Clean Air Act (ensuring emissions from manufacturing processes, such as paint booths or boilers, meet air quality standards and obtaining any necessary air permits through the Indiana Department of Environmental Management (IDEM)) and the Clean Water Act (managing wastewater discharges or stormwater runoff under the appropriate permits to protect waterways). The plant will also properly manage hazardous wastes in compliance with the Resource Conservation and Recovery Act (RCRA) and adhere to the Toxic Substances Control Act (TSCA) for any chemical substances used in production. Furthermore, Honda meets the requirements of the Emergency Planning and Community Right-to-Know Act (EPCRA) by maintaining up-to-date records of hazardous chemicals on-site and reporting as required to local emergency planners and responders. All environmental permits and records are maintained meticulously, and compliance inspections or audits are welcomed as opportunities to verify and improve adherence.

- **Environmental Risk Management:** Beyond basic compliance, Honda proactively identifies and manages environmental risks associated with its operations. This includes assessing risks of spills, accidental releases of pollutants, excessive air emissions, or other environmental incidents. The plant has controls and contingency plans in place to prevent and respond to such events—for example, spill containment systems and response kits for oil or chemical leaks, emission control devices and routine maintenance to prevent air pollution exceedances, and fail-safes in wastewater treatment systems to avoid unauthorized discharges. Regular environmental audits and risk assessments are conducted to evaluate potential weak points in environmental controls. By managing these risks, Honda protects the environment and reduces the likelihood of regulatory violations or community impacts.

- **Data Management and Reporting:** Honda tracks environmental performance data and complies with all required environmental reporting. This includes monitoring air emissions (including Carbon Dioxide, levels of volatile organic compounds from paint operations or other regulated pollutants) and water discharge quality on a continuous or periodic basis. The plant maintains detailed records of waste generation, chemical inventory and usage, and any environmental incidents. Honda submits required reports such as annual emissions inventories, Toxic Release Inventory (TRI) data if applicable, Tier II hazardous chemical inventory reports under EPCRA, and discharge monitoring reports for wastewater permits. Accurate data management and timely reporting ensure transparency with regulators and the public, and they help the company measure progress toward environmental goals.

- **Technological Support:** The plant leverages technology to support environmental compliance and performance. For example, continuous emissions monitoring systems (CEMS) might be used on certain equipment to provide real-time data on air emissions. Sensors and automation in wastewater treatment can monitor pH, chemical levels, or flow rates and alert staff to any out-of-range conditions. Environmental management software may be used to track permit requirements, due dates for inspections or trainings, and to store documentation (in the form of safety data sheets, inspection records, and regular auditing). By using modern technology and data analytics, Honda can more effectively identify trends (such as a gradual increase in energy or water usage) and target opportunities to reduce environmental impact. Technology also helps in early detection of potential compliance issues so that they can be corrected before becoming problems.

1.9 Supply Chain Management

A resilient and compliant supply chain is critical to uninterrupted production at the Honda plant. Honda's supply chain management efforts include:

- **Supply Chain Risk Assessment:** The company identifies and assesses risks throughout its supply chain that could disrupt production or impact compliance. This involves evaluating suppliers and logistics for potential points of failure. Examples of risks include over-reliance on single-source suppliers for key components, suppliers located in regions prone to natural disasters or political instability, quality control issues at a vendor that could lead to defective parts, or even cybersecurity vulnerabilities at a supplier that could affect Honda's systems (via compromised parts or data exchange). Each supplier or material is reviewed for risks such as late deliveries, capacity issues, or financial instability.

- **Risk Mitigation and Continuous Monitoring:** For significant supply chain risks identified, Honda implements mitigation strategies and continuously monitors the situation. Mitigation can include qualifying multiple suppliers for critical parts (to avoid single points of failure), maintaining safety stock or buffer inventory for components with long lead times, and working closely with suppliers on quality improvement programs. Honda also stays vigilant by monitoring supplier performance metrics and external indicators (like market reports or news that might signal a supplier problem). Through regular communication with key suppliers and the use of supplier management tools, the plant keeps an eye on supply chain health in real time. This way, if a potential disruption is looming (for example, a supplier hinting at capacity issues or financial troubles), Honda can proactively adjust its plans or source alternatives.

- **Regulatory Compliance in Sourcing:** Honda will identify and adhere to any regulatory requirements that apply to its sourcing and materials. For instance, if the manufacturing process involves materials that fall under specific legal regulations (such as conflict minerals like tin, tungsten, tantalum, and gold, which require due diligence and reporting under

U.S. law), the company ensures those requirements are met. Additionally, import/export regulations, trade compliance (including tariffs or restricted trade partner screening), and environmental or safety regulations related to materials (like restrictions on hazardous substances in parts) are all considered when selecting suppliers and materials. By ensuring that sourced parts and materials comply with relevant laws and standards, Honda avoids legal complications and upholds ethical sourcing principles.

- **Supplier Compliance and Internal Controls:** The company conducts due diligence to ensure suppliers meet Honda's standards and comply with relevant laws. This may include requiring suppliers to sign codes of conduct or contractual clauses affirming compliance with labor laws, environmental regulations, quality standards, and cybersecurity practices. Honda might request audits or certifications from high-risk suppliers (for example, verifying that a supplier's facility meets ISO 9001 quality management standards or that they maintain proper cybersecurity controls if they handle Honda's data). Internally, Honda maintains controls such as approved supplier lists (only doing business with vetted suppliers), regular supplier performance reviews, and a process for addressing any supplier non-compliance or incidents. If a supplier is found to violate critical compliance requirements or to pose excessive risk, Honda will take corrective action, which could include helping the supplier improve or phasing out that supplier. These internal controls and supplier management practices ensure that the supply chain remains robust, ethical, and aligned with Honda's compliance obligations.

1.10 Data Privacy & Security

Protecting sensitive data and maintaining robust cybersecurity is vital for Honda's operations. Key elements of the plant's data privacy and security strategy include:

- **Sensitive Data Identification and Mapping:** Honda identifies all forms of sensitive data that the plant handles. This includes intellectual property (such as vehicle designs or proprietary manufacturing processes), confidential business information (production volumes, pricing, strategic plans), personal data of employees (HR records, health information) or customers, and any other critical information assets. The flow of this data through the organization is mapped out—detailing where data is collected, how it is stored and processed, and where it is transmitted or shared (including with external partners or Honda headquarters). Understanding data flows and storage locations allows the company to pinpoint vulnerability points and apply appropriate safeguards at each step.

- **Privacy and Data Protection Compliance:** Honda ensures compliance with all applicable data privacy laws and regulations. While the Indiana plant primarily operates under U.S. law, Honda takes into account relevant federal and state regulations. For example, if any personal information of consumers is collected (such as customer data for vehicle telematics or marketing), Honda will comply with the California Consumer

Privacy Act (CCPA) regarding notice, data use, and honoring consumer rights for California residents. If the business involves handling financial customer data (for instance, through any vehicle financing programs or credit applications), the plant will follow the data safeguard requirements of the Gramm-Leach-Bliley Act (GLBA). Additionally, Indiana's data breach notification law is adhered to: in the event of a data breach involving personal information, Honda must notify affected Indiana residents and the state Attorney General within the required timeframe. On a broader scale, Honda is mindful of international standards such as the EU's General Data Protection Regulation (GDPR) when dealing with any global data to ensure proper consent, data handling, and cross-border transfer practices. Regular internal audits and reviews are conducted to verify that data is being handled in accordance with these laws and Honda's own privacy policies.

- **Security Framework and Standards:** Honda's cybersecurity program at the plant is built on industry best practices and frameworks. The company aligns its security controls with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and incorporates standards from ISO/IEC 27001 for information security management. These frameworks guide the plant in covering all aspects of cybersecurity: identifying assets and risks, protecting systems with appropriate safeguards, detecting security events, having incident response plans (respond), and establishing recovery plans for continuity. Furthermore, if any operations involve U.S. government data or contracts, Honda will implement the required security controls (for example, complying with NIST SP 800-171 for protecting controlled unclassified information in government-related projects). Embracing these recognized frameworks provides a comprehensive and systematic approach to managing cybersecurity risks.

- **Zero Trust Architecture:** The plant employs a Zero Trust security architecture. In practice, this means that no user or device is inherently trusted, even if it is within the corporate network. Every access request to resources (applications, databases, network segments) is continuously verified—users must authenticate (preferably with multi-factor authentication) and be authorized for the specific action or data each time. Network segmentation is used to isolate sensitive systems, and additional verification (such as device security posture checks) is required before granting access. By assuming that threats can exist both inside and outside the traditional network perimeter, the Zero Trust approach greatly reduces the risk of an insider threat or a compromised account moving laterally across systems.

- **Access Controls and Least Privilege:** Honda enforces strict access control measures to ensure that employees and systems only have the minimum access necessary to perform their duties. This principle of least privilege is applied to user accounts, system accounts, and even application permissions. Access to sensitive systems (like financial data, confidential design documents, or critical production controls) is limited to authorized personnel based on role, and those access rights are reviewed regularly. Strong authentication mechanisms (including passwords that meet com-

plexity requirements and multi-factor authentication for remote or high-privilege access) are in place to prevent unauthorized access. When employees change roles or leave the company, their access rights are promptly adjusted or revoked as part of an off-boarding procedure.

- **Data Encryption:** All sensitive data is protected through encryption both in transit and at rest. For data in transit, Honda uses secure communication protocols such as HTTPS/TLS for web traffic, secure shell (SSH) for remote admin access, and VPN tunnels for any remote connections to the plant's network. This prevents eavesdropping or interception of data as it flows between systems. For data at rest, technologies like full-disk encryption on laptops, encryption of databases and file systems on servers, and encrypted backup media are employed. This means that if a device or storage media were to be lost or stolen, the data would remain unreadable and protected from unauthorized access.
- **Data Loss Prevention:** To prevent the unauthorized leakage of sensitive information, Honda utilizes Data Loss Prevention (DLP) measures. These include software tools that monitor and control the transfer of data through various channels (such as email, USB drives, or web uploads). If, for example, an employee attempts to send out a file containing confidential plans or export a large amount of production data, the DLP system can detect this based on content scanning and either block the action or flag it for the security team's review. DLP policies are configured to balance security with business needs, ensuring that legitimate data sharing is allowed while risky or non-compliant transfers are stopped.
- **Secure Storage and Communications:** The plant uses secure methods for storing and sharing information. Important files and intellectual property are stored in access-controlled repositories or document management systems that track versions and access history. When sharing sensitive data with suppliers or partners, Honda employs secure file transfer solutions or encrypted email rather than sending data over open channels. Within the manufacturing facility, any network-connected equipment or Internet of Things (IoT) devices are secured to prevent them from becoming entry points; this may include using segregated networks for certain equipment and ensuring firmware is kept updated. Overall, communications that involve sensitive or proprietary information are protected so that eavesdropping or tampering is prevented.
- **Employee Training and Awareness:** Human awareness is a critical component of data security. Honda provides regular training to employees about cybersecurity best practices and data protection. This includes educating staff on how to recognize phishing emails or social engineering attempts, proper use of company devices, secure password creation and management, and the importance of reporting suspicious incidents promptly. Specialized training is given to those in high-risk roles (for instance, IT administrators or those handling sensitive data) to ensure they understand the specific threats and responsibilities they have. By fostering a culture of security awareness, the plant reduces the likelihood of accidental security breaches and empowers employees to act as an additional line of defense.

- **Incident Response and Recovery Plans:** Despite all preventive measures, Honda prepares for the possibility of cybersecurity incidents or data breaches. A documented Incident Response Plan (IRP) is in place, which outlines the steps to be taken in the event of a security incident—such as a malware outbreak or detected data breach. The IRP defines roles (such as who is on the response team), communication channels (how to escalate issues to management and, if needed, to law enforcement or affected parties), and procedures for containment, eradication of threats, recovery of systems, and post-incident analysis. In conjunction, a Disaster Recovery Plan (DRP) exists to address how the plant would restore critical operations and data in case of a major disruptive event (cyber-related or even physical disasters). This includes regular backups of key systems and data, off-site storage of backups, and drills or simulations to test recovery times. Together, these plans ensure that Honda can respond swiftly to incidents, minimize damage, and recover normal operations as quickly as possible.

- **Security Audits and Vulnerability Management:** The plant undergoes regular security audits and continuous vulnerability management. Security audits (internal and occasionally external) review the effectiveness of controls and compliance with policies. For example, an audit might check that firewall rules are properly set, user accounts are managed correctly, or that security cameras and access controls are functioning in restricted areas of the facility. On the technical side, Honda employs vulnerability scanning tools that routinely scan the network, servers, and applications for known vulnerabilities or misconfigurations. Critical systems are also subject to periodic penetration testing to simulate attacks and uncover any weaknesses that scanners might not catch. When vulnerabilities are identified—whether through scanning, reported by employees, or via threat intelligence about software used at the plant—there is a process to prioritize and apply patches or remedial actions promptly. Keeping systems updated and hardened is an ongoing effort in the security program.

- **Monitoring and User Activity Logging:** Finally, continuous monitoring is a cornerstone of Honda's security posture. The plant uses security information and event management (SIEM) systems to aggregate and analyze logs from various sources: network devices, servers, workstations, and security appliances. Alerts are configured to notify the security team of unusual patterns (such as repeated failed logins, after-hours access to sensitive systems, or unrecognized devices connecting to the network). Critical systems and areas are monitored via surveillance and alarms to detect any physical intrusion or unauthorized access. Additionally, user activity on sensitive systems is logged and periodically reviewed to ensure that employees are adhering to policies and not engaging in risky behavior. This monitoring respects privacy laws and focuses on detecting genuine threats or misuse. By maintaining vigilant monitoring and timely review of security events, Honda can quickly detect, investigate, and respond to potential security issues before they escalate.

Chapter 2

Acceptable Use Policy

2.1 Purpose

The purpose of this Acceptable Use Policy (AUP) is to protect the confidentiality, integrity, and availability of Honda's technology resources, including computer systems, networks, and data. This policy establishes guidelines for the appropriate use of these resources to ensure they are used securely and responsibly. By defining acceptable and unacceptable uses, Honda aims to safeguard its operations from risks such as data breaches, malware infections, and other potential security incidents.

2.2 Scope

This policy applies to all individuals who use or have access to Honda's information technology resources. This includes, but is not limited to:

- All Honda employees (full-time, part-time, and temporary staff).
- Contractors, consultants, and other third-party workers providing services to Honda.
- Visitors and external partners (such as vendors or suppliers) who are granted access to Honda's IT systems or networks, including those at any Honda facility or plant.

Everyone covered under this scope is required to understand and abide by the rules outlined in this AUP whenever accessing company-owned devices, networks, or data.

2.3 Acceptable Use

Honda's computing devices, network, internet access, and other IT resources are provided to support business operations and should be used primarily for legitimate company purposes. Users are expected to exercise good judgment and use these resources in an efficient, ethical manner aligned with Honda's business goals. Limited personal use of IT resources is allowed as long as it does not

interfere with one's job responsibilities, does not degrade network performance, and does not violate any policies or laws. Examples of acceptable use include:

- Using company email and messaging systems for professional communication with colleagues, clients, and partners.
- Accessing the internet for work-related research, online training, and other business-related information.
- Utilizing business software applications and tools provided by Honda for your role (such as data analysis, project management, customer service platforms).
- Incidental personal use (such as briefly checking personal email or news during a break) that does not hinder work duties or security.

2.4 Unacceptable Use

Any behavior that falls outside the scope of acceptable use is prohibited. The following actions are considered unacceptable and strictly forbidden for anyone using Honda's IT resources:

- Attempting to gain unauthorized access to any Honda system, network, application, or data (hacking or otherwise attempting to gain unapproved access to company computers, accounts, or systems).
- Downloading, uploading, or distributing illegal content or unlicensed/pirated materials, including software, media, or documents.
- Knowingly introducing or propagating malicious software (such as viruses, worms, or spyware) or engaging in any activities that could compromise network security.
- Engaging in activities that violate intellectual property rights or copyright laws, such as sharing copyrighted material without permission or using unapproved software.
- Sharing your Honda passwords or accounts with others, or failing to follow Honda's password requirements (such as using weak passwords or reusing corporate credentials on external sites).
- Using Honda's IT resources to engage in unlawful activities or to harass, bully, or defame any individual or group.

Unacceptable use of company resources will result in disciplinary action as outlined in this policy. When in doubt about whether an action is allowed, users should seek guidance from a supervisor or the IT department before proceeding.

2.5 User Responsibilities

Every authorized user of Honda's IT resources is expected to uphold the following responsibilities to maintain a secure computing environment:

- **Adherence to Password Policy:** Create and use strong passwords in accordance with Honda's Password Policy. Passwords must remain confidential and should never be shared. Users are required to change passwords periodically as directed by policy.
- **Incident Reporting:** Promptly report any suspected security incidents, breaches, or policy violations to Honda's IT security team or helpdesk. This includes reporting things like unexpected system behavior that might indicate malware, or any loss/theft of devices.
- **Data Protection:** Handle sensitive and confidential data with care. Use company-approved encryption solutions for storing or transmitting sensitive information, and follow Honda's data backup procedures and retention guidelines. Do not copy or store company data on unapproved personal devices or cloud services.
- **General Security Practices:** Be vigilant and exercise good cybersecurity hygiene. This includes keeping your devices updated with the latest security patches, running antivirus scans as required, and not disabling or interfering with security features installed on your systems.

By fulfilling these responsibilities, users help protect both themselves and the company from security threats.

2.6 Monitoring and Enforcement

Honda reserves the right to monitor and log all usage of its IT systems and network to ensure compliance with this policy and other security requirements. Users should be aware that there is no guarantee of personal privacy when using company resources; any data created, stored, or transmitted on Honda systems may be reviewed by authorized personnel. Monitoring methods may include automated tools and manual audits of network traffic, email, and file storage.

If any activity in violation of this AUP is detected or suspected, Honda will take the following steps:

- **Investigation:** The IT security team or authorized personnel will investigate the potential violation. This may involve reviewing log files, examining the content in question, and conferring with the user's manager.
- **Access Suspension:** During an investigation, a user's access to certain systems may be temporarily suspended to protect company resources and preserve evidence.
- **Review and Determination:** Upon concluding the investigation, management (in consultation with HR and IT security) will review the findings. If a violation is confirmed, an appropriate disciplinary action will be determined in line with company policies (see Section 2.9).
- **Enforcement:** Confirmed violations will result in enforcement of consequences as described in this policy. All actions taken will be documented, and the outcome will be communicated to the involved parties.

Through these monitoring and enforcement measures, Honda aims to deter improper use and promptly address any issues that arise.

2.7 Software Installation Rules

To maintain a secure and standardized computing environment, users are not allowed to install or use unauthorized software on Honda-owned devices:

- Only software that has been approved by Honda's IT department may be installed on company computers and devices. Users must not download or run any freeware, shareware, or third-party applications that have not been vetted and authorized.
- Installation of personal software, games, or any unlicensed applications on company devices is strictly prohibited. If a specific software tool is needed for business purposes, employees should request it through the official IT procurement or helpdesk process.
- Users should not attach or install any unauthorized hardware or peripherals (USB drives of unknown origin, personal network equipment, etc.) to company systems, as these could introduce security vulnerabilities.

These rules ensure that all software running on Honda systems is properly licensed, up-to-date, and secure.

2.8 Supply Chain Security

Honda recognizes that security extends to its relationships with vendors and suppliers. All supply chain partners must adhere to the following guidelines to maintain the security of Honda's operations:

- **Vendor Compliance:** Vendors, suppliers, and contractors must comply with Honda's security policies and procedures when accessing Honda facilities, networks, or data. This requirement should be included in all relevant contracts and agreements.
- **Cybersecurity Assessments:** Honda may require vendors to undergo cybersecurity risk assessments or provide proof of their own security measures. Partners with access to Honda's critical systems or sensitive data should meet defined security standards and may be subject to periodic security reviews or audits.
- **Physical Delivery Controls:** Deliveries of equipment, products, or materials from external partners must be made only to authorized locations (for example, the facility's Receiving department). All incoming shipments and vendor visits should follow Honda's physical security protocols, including sign-in procedures and escort policies if required.
- **Secure Integration:** Any hardware, software, or services provided by a vendor that will be integrated into Honda's environment must be approved by Honda's IT and security teams. Such components should be reviewed for security vulnerabilities and compliance with Honda's standards before deployment.

By enforcing supply chain security measures, Honda helps ensure that third-party relationships do not introduce unacceptable risk to its own networks and data.

2.9 Consequences and Violations

Violations of this Acceptable Use Policy are taken seriously and can lead to disciplinary action. All incidents of non-compliance will be reviewed on a case-by-case basis, and consequences will be applied appropriate to the severity of the offense. The following table provides examples of violation levels and their typical consequences:

Violation Severity	**Typical Consequences**
Minor or unintentional violation (accidental breach of policy with no harm intended)	Coaching or a verbal/written warning, along with additional training on proper use and security policies.
Serious or repeated violation (willful misconduct, causing security breach, or multiple offenses)	Formal disciplinary action up to and including termination of employment. Legal action may be pursued in cases involving unlawful activities or serious negligence.

Table 2.1: Examples of AUP Violations and Consequences

Ultimately, any employee or user found to be in violation of this policy will be held accountable. Disciplinary measures will be carried out in accordance with Honda's human resources policies and may impact the individual's employment status. By enforcing these consequences, Honda maintains a strong security posture and encourages all users to follow the rules and best practices outlined above.

Chapter 3

Password Policy

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Chapter 4

Security Awareness Training

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Chapter 5

Web Application Security

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Chapter 6

Software Compliance

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Chapter 7

Bring Your Own Device (BYOD)

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Chapter 8

Clean Desk Policy

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Chapter 9

Email Security

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Chapter 10

Third-Party Security

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Chapter 11

Server Security

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Chapter 12

Remote Access

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Chapter 13

Encryption Policy

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

Chapter 14

Firewall Policy

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Chapter 15

Network Diagram

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

Chapter 16

Disaster Recovery Policy

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam congue neque id dolor.

Chapter 17

Artificial Intelligence (AI) Policy

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

Chapter 18

Additional Policies (TBD)

Nulla non mauris vitae wisi posuere convallis. Sed eu nulla nec eros scelerisque pharetra. Nullam varius. Etiam dignissim elementum metus. Vestibulum faucibus, metus sit amet mattis rhoncus, sapien dui laoreet odio, nec ultricies nibh augue a enim. Fusce in ligula. Quisque at magna et nulla commodo consequat. Proin accumsan imperdiet sem. Nunc porta. Donec feugiat mi at justo. Phasellus facilisis ipsum quis ante. In ac elit eget ipsum pharetra faucibus. Maecenas viverra nulla in massa.