HONDA

2025 Security Policy

Office of Information Technology
Security Department

Greensburg, Indiana
June 6, 2025

Table of Contents

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 Greensburg, 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, 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, including data security & privacy, quality control, and occupational safety to environmental protection and supply chain oversight. Defining this scope ensures that GRC efforts remain focused on relevant areas and do not become overly broad or unmanageable.

1.3 Roles and Responsibilities

While many employees interact and operate within the policy standards defined within this document, those held accountable for the effectiveness, maintenance, and audit of policies held within the Honda Security Policy are detailed below.

Role	**Responsibilities**
Chief Risk Officer (CRO)	Identifying, assessing, and mitigating risks that may impact Honda's financial operations and reputation.
Chief Information Security Officer (CISO)	In charge of all aspects of security within Honda, including data protection, cybersecurity, and IT security.
Compliance Officer	Ensures that Honda adheres to all applicable laws, regulations, and industry standards.
Security Analyst	Responsible for the technical aspects of cybersecurity within Honda, including network monitoring and threat detection.

Table 1.1: Roles and Responsibilities in Risk and Security Management

1.4 Establishing Policy

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

1. **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 instill a culture of integrity throughout the organization.

2. **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.

3. **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.

4. **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.

5. **Annual Review & Renewal** Honda will review and renew it's Incident Response, Business Continuity, Disaster Response, and Security Policy annually. This process ensures that Honda is able to adapt to current threats, regulations, and allow for the implementation of the latest established best-practices.

1.5 Risk Management

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

1. **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). For further information, refer to the Business Continuity Policy.

2. **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. For further information, please reference the Incident Response Policy.

3. **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, adjusting 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. For further information, please reference the Business Continuity Policy.

1.6 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	**Definitions & 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 di- rectories.*
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 pro- duction 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*

Table 1.2: Data Classification Matrix

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.

1.7 Data Retention

Honda will retain customer, internal, and partner data for no longer than a period of seven years. While there is currently no applicable laws governing the retention of data in Indiana, federal and global legal regulations are constantly changing, and in anticipation of future changes; Honda reserves the right and obligation to store data for legal purposes. This includes but is not limited to:

1. **Customer Data** is considered to be any data related to the transfer of information between Honda and it's customers. This can include personal information, including potentially personally identifiable information.

2. **Financial Data** is considered to be any data related to the transfer of money between Honda and it's partners, customers, and suppliers. This can potentially consist of restricted or confidential information that must be handled differently than publicly available information.

3. **Environmental Data** is considered to be any data that relates to any information gathered about Honda's effect on the environment, including markers like pH levels, chemical contaminants, spills, and carbon dioxide emissions or potentially toxic fumes.

4. **OHS Data** is considered to be any data that is collected in relation to the health and well-being of Honda's employees. This may include information such as injury rates, safety training effectiveness, etc.

5. **Network Data** is considered to be any data that is generated from activity on Honda's network, most commonly network logs collected from employee or corporate devices.

1.8 Data Destruction

All applicable data no longer in retention or in-use by Honda is applicable for destruction. After retained data no longer needs to be held, it will be manually destroyed by the Security Team. The Data Destruction Policy must be followed to maintain confidentiality of sensitive data; including but not limited to cryptographic erasure, degaussing, and/or physical destruction of storage technology where applicable.

1.9 Quality Management

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

1. **Incoming Raw Material Inspection:** All incoming raw materials and components are subject to stringent quality checks before they enter production. Inspection of materials will be determined by state guidelines, following department of transportation recommendations, (namely, the Manual For Frequency of Sampling and Testing and Basis For Use of Materials)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.

2. **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.

3. **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.

1.10 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:

1. **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.

2. **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.

3. **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.

4. **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 annually. 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. Training is to be done semi-annually for employees in low-risk environments, and bi-monthly for employees in high-risk environments. Employees who fail to meet training expectations and/or safety evaluations will be suspended and given remedial training or be reviewed for termination.

5. **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.

1.11 Environmental Management

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

1. **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. Honda will review it's environmental compliance standards monthly, and after every applicable incident concerning environmental factors (such as water quality, air quality, or threats to public health).

2. **Environmental Risk Management:** Beyond basic compliance, Honda proactively identifies and manages environmental risks associated with its operations as per the Disaster Recovery Policy.

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. Monthly 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.

3. **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.

4. **Technological Support:** The plant leverages technology to support environmental compliance and performance. For example, continuous emissions monitoring systems (CEMS) will be used on specified equipment (as per the Environmental Protection Policy) 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.

1.12 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:

1. **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. Refer to the Business Continuity Plan for more information.

2. **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.

3. **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.

4. **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.

1.13 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:

1. **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.

2. **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 seventy-two hours. 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. Semi-annual internal audits and reviews are conducted to verify that data is being handled in accordance with these laws and Honda's own privacy policies.

3. **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, 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.

4. **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 with multi-factor authentication when accessing Restricted or Confidential information 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.

5. **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 complexity requirements and multi-factor authentication as per the Password Policy) 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. An Audit of all current access controls will be done semi-annually for all user and system accounts.

6. **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 and tokenization 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. More information can be found in the Encryption Policy.

7. **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.

8. **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.

9. **Employee Training and Awareness:** Employee 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. For further information, refer to the Security Awareness Policy.

10. **Incident Response and Recovery Plans:** Despite all preventive measures, Honda prepares for the possibility of cybersecurity incidents or data breaches: therefor, Honda has mandated the creation of a Business Continuity, Disaster Recovery, and Incident Response Plans. 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. For more information, refer to the Incident Response, Disaster Recovery, and Business Continuity Plans.

11. **Security Audits and Vulnerability Management:** The plant undergoes semi-annual security audits and continuous vulnerability management. Security audits (internal and 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 annual penetration testing to simulate attacks and uncover any weaknesses that scanners might not catch. When vulnerabilities are identified, security procedures and patches will be updated or applied as per the vulnerability's applicable policy.

12. **Monitoring and User Activity Logging:** Continuous monitoring is a cornerstone of Honda's security posture. The plant uses security information and event management, including but not limited to: (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 continuously monitored 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:

1. All Honda employees (full-time, part-time, and temporary staff).
2. Contractors, consultants, and other third-party workers providing services to Honda.
3. 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. While not all-inclusive, examples of acceptable use can include:

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

Employees, visitors, and third-parties, should keep in mind that these examples do not encompass every possible example of acceptable-use. We recommend that employees, visitors, and third-parties use good judgment in their usage of company systems and resources, and to contact IT management regarding what acceptable or unacceptable use may entail.

2.4 Unacceptable Use

Any behavior that falls outside the scope of acceptable use is prohibited. While not all-inclusive, unacceptable use of Honda's IT systems & resources may include:

1. 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).
2. Downloading, uploading, or distributing illegal content or unlicensed/pirated materials, including software, media, or documents.
3. Knowingly introducing or propagating malicious software (such as viruses, worms, or spyware) or engaging in any activities that could compromise network security.
4. Engaging in activities that violate intellectual property rights or copyright laws, such as sharing copyrighted material without permission or using unapproved software.
5. 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).
6. Using Honda's IT resources to engage in unlawful activities or to harass, bully, or defame any individual or group.
7. Installing non-approved or banned software on company resources. Please refer to the Software Compliance Policy.

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 IT Management 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:

1. **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 the password policy. For more information, please refer to the Password Policy or speak with IT Management.
2. **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. If anybody requests your password, you must immediately report to the IT Security Management Team.
3. **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.
4. **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:

1. **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.

2. **Access Suspension:** During an investigation, a user's access to certain systems may be temporarily suspended to protect company resources and preserve evidence.

3. **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 2.7).

4. **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 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. While not all-inclusive, 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 gross negligence.

Table 2.1: Examples of AUP Violations and Consequences

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

3.1 Purpose

The purpose of this Password Policy is to establish a standard for the creation, protection, and management of passwords used to access systems and information. Strong passwords reduce the risk of unauthorized access to systems and data.

3.2 Scope

This policy applies to all employees, contractors, vendors, and third-party users who access company systems, networks, or data. Exceptions to this policy must be approved in writing by the Chief Information Security Officer (CISO) or designer

3.3 Password Requirements

Complexity

All passwords must meet the following criteria:

1. Minimum length: 12 characters
2. Maximum length: 36 characters
3. Must include at least three of the following:
   (a) uppercase letter (A - Z)
   (b) lowercase letter (a - z)
   (c) Number (0 - 9)
   (d) special character (e.g.,!, @, *)

Administrative passwords must also include:

1. Minimum length: 14 characters
2. Passphrase is required
3. Must use Multi-Factor Authentication

Prohibited Passwords

1. Common or easily guessed passwords. (e.g., "password123", "admin", "welcome")
2. Passwords matching the username or user ID.
3. Dictionary words without modification.
4. Passwords used in the previous 12 months.

3.4 Password Expiration and Change

1. Users will be notified 14 days prior to password expiration.
2. Temporary or initial passwords must be changed upon first login.
3. Passwords must be changed every 90 days.

3.5 Password Storage

1. Passwords must never be written down or stored in plain text.
2. Password management tools must be approved by IT.

3.6 Multi-Factor Authentication (MFA)

MFA is required for access to administrative accounts, to Remote access company systems, and to access Financial and personally identifiable information (PII) systems.

3.7 Account Lockout Policy

After 3 failed login attempts, the account will be locked for 15 minutes. After an account has been locked 3 times in a row it will remain locked and will require contacting IT to unlock.

3.8 Enforcement

Violation of this policy may result in disciplinary action, up to and including termination.

Chapter 4

Security Awareness Training

4.1 Purpose

Our Cybersecurity Awareness Training aims to establish a comprehensive framework for promoting a culture of cybersecurity awareness, knowledge, and responsible behavior throughout Honda. This policy aims to provide guidelines and procedures for developing, implementing, and continuously improving cybersecurity education and awareness programs that empower our employees to recognize, prevent, and respond to potential cyber threats. By prioritizing education and awareness, this policy seeks to enhance the overall security posture of Honda, reduce the likelihood of human error leading to security incidents, and foster a sense of shared responsibility for protecting our systems, data, and networks. Through regular training, communication, and engagement initiatives, we strive to cultivate a vigilant and resilient workforce equipped to safeguard our sensitive information and assets in the face of evolving cybersecurity risks.

4.2 Scope

The Cybersecurity Awareness Training applies to all Honda employees, contractors, vendors, and stakeholders. This policy encompasses planning, developing, implementing, and evaluating cybersecurity education and awareness programs to foster a culture of security awareness and responsible behavior. It covers training sessions, workshops, communication campaigns, and resources to enhance understanding of cybersecurity risks, best practices, policies, and procedures. The policy applies to all individuals who access Honda's network, systems, and sensitive information. Compliance with this policy is mandatory for all personnel, and active participation in cybersecurity education and awareness initiatives is required. Any exceptions or deviations from this policy require approval from the designated authority responsible for cybersecurity governance.

4.3 Safeguards

To achieve Honda's overall mission, and the purpose of this cybersecurity policy, Honda shall:

1. Ensure that all workforce members have access to the documentation defining the cybersecurity safeguards related to their roles and responsibilities.

2. Maintain a technology platform for delivering cybersecurity-related education to workforce members (such as a Learning Management System).

3. Maintain a technology platform (such as a Learning Management System) for tracking cybersecurity-related education delivered to workforce members.

4. Ensure that all workforce members (including engineers, developers, and privileged users) regularly receive appropriate education on cybersecurity safeguards related to their roles and responsibilities.

5. Ensure that all workforce members regularly receive appropriate cybersecurity awareness training that is appropriate to their roles and responsibilities.

6. Ensure that Honda's cybersecurity education program appropriately educates workforce members on securely authenticating to information systems.
7. Ensure Honda's cybersecurity education program appropriately educates workforce members on securely communicating over untrusted networks.
8. Ensure that Honda's cybersecurity education program appropriately educates workforce members on securely handling data, including the most likely reasons data may be exposed.
9. Ensure Honda's cybersecurity education program appropriately educates workforce members on securely responding to social engineering techniques, including identifying and handling such activities.
10. Ensure Honda's cybersecurity education program appropriately educates workforce members on securely reporting cybersecurity safeguard failures.
11. Ensure that Honda's cybersecurity education program appropriately educates workforce members on securely reporting potential cybersecurity incidents to Honda. If you see something, say something.
12. Regularly perform educational activities that reinforce Honda's cybersecurity education program and validate the effectiveness of the program such as an email phishing campaign.
13. Regularly report the results of the validation of the effectiveness of Honda's cybersecurity education program to business stakeholders.

4.4 Enforcement

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.

Chapter 5

Web Application Security

5.1 Purpose

The purpose of Web Application Security is to ensure and ensure that all Web applications that have been developed, currently deployed, or maintained by Honda are secure. The customer-facing side, internal systems, and third-party developer resources all must be maintained and kept secure while minimizing security vulnerabilities. This policy aims to protect customer and internal data; while also complying with any regulatory standards or laws, and reducing risks pertaining to cyber attacks (data breaches or disruption of any services). The purpose of this project is to ensure that there are clear roles, responsibilities, and processes for application security and protection of these web assets.

5.2 Scope

Honda's Web Application Security Policy is in place to keep the organization's Web Applications safe and protected from cyber threats. This policy applies to employees or members of Honda; and all who use or access Honda's online resources, online (cloud-based) or in person (local). As well as third parties or contractors who maintain or use the company's databases and servers. These third parties must take all necessary precautions when using Honda's resources. Vendors involved in software development, testing, deployment, or monitoring/maintenance must also comply. In addition, this policy applies to all web applications, whether they are for vendors, customers, or internal uses; if developed or used by Honda, they are included.

5.3 Roles and Responsibilities

To ensure the security of web applications, collaboration is a much-needed resource, stretching across many departments and roles.

5.3.1 Developers

1. Developers implement secure coding and best practices using industry standards for security such as OWASP (Open Worldwide Application Security Project) which provides many security standards for web applications.

2. Participation in secure code reviews, threat modeling sessions, and security training. This allows them to stay up to date with current security practices, while also ensuring that others are competent and following security procedures.

3. Observe and fix and security issues identified while being within the SLA (Service Level Agreements) timeframe. The response time and resolution time must be met to ensure security concerns and maintain good relations with customers or users. These SLA Time frames will vary on the type and severity of the problem, but the developers should still fix to the time frame given.

5.3.2 Security Team

1. Establish and maintain security tooling and controls (scanners, firewalls, Web application firewalls). Security tooling, updating of software and security software, reviewing any configurations or changes that must be made, and validating and testing whether these tools and softwares are able to combat current and evolving threats.

2. Conduct regular audits, penetration tests, and risk assessments. Doing so, ensures the current security of the system and how well responses will be to current and evolving threats.

3. Oversee security awareness and training for application teams, ensuring that all members are up to date on any needed information or training. While also ensuring that employees are competent.

5.3.3 Devops/Infrastructure Teams

1. Integrate security checks in CI/CD (Continuous Integration and Continuous Delivery/Delivery) pipelines (Static Application Security Testing and Dynamic Application Security Testing). CI/CD pipelines is a workflow system, oftentimes having steps such as the Source Stage, Build Stage, Test Stage, Deploy Stage, and Monitor Stage.

2. Enforce deployment rules for production access and configurations. Enforcement of these will ensure a high level of security and reliance if these are all followed.

3. Maintain secure system images and infrastructure code or systems. Maintaining and monitoring these ensures up to date and secure systems.

5.3.4 Quality Assurance and Testing Teams

1. Validate security features and protections as part of test plans. Testing these features ensures that everything is up to date and can protect systems against current cyber threats.

2. Use automated testing tools to detect common vulnerabilities (XSS, SQL injections). Doing so regularly will ensure the systems are in place and that they are ready for any current or future evolving threats.

3. Ensure that security test cases are included in test cycles.

5.3.5 Third Parties

1. Make sure they follow Honda's secure development and operational policies at all times. This will ensure that those involved with Honda do not cause any operational or security concerns.

2. Undergo periodic security assessments. These third parties will go through security checks every quarter and provide logs of anything and everything they were doing with Honda's resources and web applications.

3. Notify Honda of any security breaches or suspected vulnerabilities in shared platforms. Third parties will be required to report any security breaches or flaws they find in a timely and professional manner. As well as reporting any vulnerabilities they find.

5.4 Security Requirements

5.4.1 Secure Development Lifecycle (SDLC)

Security must be included and integrated into every stage of the application lifecycle—from its requirements to deployment.

1. All involved teams must follow a documented Secure SDLC process that includes:

2. Planning and security requirement definition

3. Threat modeling and risk assessment

4. Secure coding practices/ secure development (input sanitization or access control)
5. Security testing prior to each release to ensure secure deployment
6. Honda and its partners are sticking to coding rules that match up with OWASP, MITRE CWE, and CERT guidelines.
7. The dev teams need to keep up with training to stay aware of new threats including how to address and fix them.

5.4.2 Authentication and Authorization

Access to web applications and their resources must be strictly controlled to ensure only legitimate users perform authorized actions.

1. All users must authenticate using strong credentials and MFA where applicable. Proper security precautions for users are required to ensure that access to systems can't be exploited through passwords or any user information.
2. Single Sign-On (SSO) using OAuth 2.0, OpenID Connect, or SAML must be implemented across corporate systems. This simplifies the process and speeds up the authentication process by making the user only have to be authenticated the first time they login within a single session.
3. Sessions must expire after a predefined period of inactivity (default: 15–30 minutes). Session expiration is a crucial security feature that must be implemented at all stages. This expiration is for systems to not be interacted with by unintended users while a system is left inactive.
4. Tokens must be securely stored (e.g., HTTPOnly, SameSite, Secure flags). These tokens are important to authentication and are needed to have in place only for users who have these permissions and are authorized.
5. Access permissions must be role-based and reviewed quarterly to eliminate excess privilege (least privilege enforcement). Essentially, the roles that are assigned to users need certain permissions, or systems that have permissions, only are granted the minimum level of access necessary to complete their work or current roles.

5.4.3 Input Validation

Improper handling of user input is a leading cause of application vulnerabilities. The proper handling of these inputs is a crucial part for security.

1. All input must be validated against a strict schema, or having any data or information is needed to be formatted to a predetermined pattern, format, or structure. . It is preferred to use allow-lists or only accept known safe characters or formats.
2. Sanitize all inputs; remove or alter any data that may be harmful to the system, especially those that interact with databases, file systems, or OS This is to prevent cyber attacks such as SQL injections.
3. Client-side validation may improve user experience but cannot replace server-side validation. Both are in place; client-side for user experience, and server-side to ensure that all data is correct and all validations are in true.
4. To prevent any injection attacks (HTML injection, cross-site scripting, XML injection, etc) , any output should be contextually encoded before being shown to other environments. (HTML, JavaScript, JSON, XML)

5.4.4 Data Protection

Data confidentiality and integrity must be ensured through all encryption and access control mechanisms.

1. All data in any type of transit must use Transport Layer Security (TLS 1.2 or higher) to protect against eavesdropping and man-in-the-middle attacks.
2. Sensitive data at rest such as credentials or payment data must be encrypted using approved algorithms like AES-256, a 256-bit encryption.
3. Passwords must never be stored in plaintext and must be hashed using secure algorithms. This ensures proper secure storage of these passwords that keep them secure even if someone gains access to the list of them.
4. Encryption keys must be rotated periodically and stored securely (e.g., using AWS KMS, Azure Key Vault, or HSMs). The time between each rotation is up to the current security regulations (once a year). Constant use of a key requires it to be changed often to prevent any compromises.

5.4.5 Secure APIs

APIs are a common attack vector and must be treated with the same security rigor as the front-end.

1. All APIs (Application Programming Interface) must require authentication, ideally through OAuth 2.0 access tokens or mutual TLS. These authentications confirm whether or not whoever interacts have proper permissions.
2. Implement proper authorization checks on every endpoint (not just at the gateway). Thus preventing any unauthorized access, ensuring that only proper authorized individuals can make any changes to any part of the system.
3. Use rate limiting and API throttling to prevent abuse or denial-of-service attacks. This practice controls the rate of requests to the network or server. This places a hard limit to requests in a window of time, allowing for proper share and fair resource usage as well.
4. APIs must never expose internal implementation details or stack traces. These details or traces can have potential private or sensitive information such as paths of files, source code, information of the systems or databases, user credentials, and access tokens are all examples.

5.5 Security Testing and Monitoring

5.5.1 Static and Dynamic Testing

1. **Static Application Security Testing (SAST)** tools must be integrated into CI/CD (Continuous Integration and Continuous Delivery/Delivery) workflows to detect code-level issues early.
2. **Dynamic Application Security Testing (DAST)** must be used on deployed environments to uncover issues such as broken authentication or logic flaws.
3. All testing must generate reports with severity levels and the steps following anything found during these tests. The severity levels will determine the response, the response time, and the individuals assigned to the problem or incident.

5.5.2 Penetration Testing

1. Internal or third-party red teams must conduct penetration tests at least annually. These tests must be done on a safe platform to not disrupt business.
2. Penetration testing must simulate real-world threat actors and tactics to evaluate defense mechanisms. The ever changing and evolving cyber-threats require the most up to date training to maintain high levels of security.

3. All findings must be categorized by risk level, assigned to owners, and tracked to closure. These risk levels will assign the severity of the problem and how fast it is needed to be fixed to remove any vulnerabilities. The complete tracking and documentation of these findings are crucial to understand anything and everything affected, and to plan for any follow-up changes that may need to be made.

4. Testing must be performed before major product launches or infrastructure changes. This testing is done during these times to ensure that all products are as safe as possible with no vulnerabilities before releasing the public or anyone connected to Honda. Testing before infrastructure changes are to upkeep security and will allow for any vulnerabilities to be addressed before major changes.

5.5.3 Vulnerability Management

1. All code repositories and dependencies must be scanned regularly using reliable tools. These scans are to ensure regular and constant security measures are up and in place and there are no vulnerabilities that can be exploited.

2. Critical vulnerabilities must be patched or mitigated within 7 business days; medium vulnerabilities within 30 days. These timeframes are set in place to not disrupt or halt business and to have the system as safe as possible at all times.

3. Unused components and features must be removed from applications to reduce the attack surface. Unused components and features are best removed to not slow down monitoring and upkeep. If anything is unused, remove promptly with correct procedures and documentation. The less unknown features that can be exploited, the higher the security

5.6 Logging and Monitoring

1. Applications must generate detailed logs for access attempts, privilege changes, data exports, and error conditions. These logs keep track of all interactions with the applications.

2. Logs must be protected against unauthorized access and tampering. The logs must only be able to be accessed by authorized personnel.

3. Use centralized log aggregation and analysis tools (ELK Stack, Splunk, etc) for real-time alerting. These tools will keep track of all actions, also they will have resources such as rapid detection, real-time analysis, improved security, improved scalability, and have visualization tools that help teams to easily monitor systems in an easy to understand model

4. baselines and rules for detecting abnormal behavior (login anomalies, privilege escalation). These baselines are in-place to ensure that no behavior may slip past, any and all related abnormal behaviors will be logged for security reasons.

5.7 Incident Response

1. All applications must be covered under Honda's Incident Response Plan (IRP), with clear contacts for escalation. These incidents can take place at any time and at any level, security precautions at every point are to guarantee appropriate responses will be available no matter where and when a problem may arise.

2. Some of these incident categories may include unauthorized access, data leakage or breaches, denial of service, and compromise of the system to gain a level of control over it.

3. All teams must understand their role in incident detection, containment, communication, and recovery. This understanding is in place to skip and fast-track the process of reaction without needing to assign personnel to certain actions, they will already have and know their role.

4. Post-incident reviews must include root cause analysis and follow-up actions to prevent recurrence. The documentation of incidents is crucial, with the information fully laid out with a follow-up plan is the most important part. The ability to understand what went wrong and where allows for the planning of how the future will be and any policies or systems that will need to be updated.

5.8 Third-Party and Open Source Components

1. Teams must maintain an inventory of all third-party components and their versions (a Software Bill of Materials). Essentially, it is a list of all the inventory of everything such as components, libraries, and dependencies.

2. Libraries must be updated regularly, especially those with known CVEs (Common Vulnerabilities and exposures).This is to ensure and keep track of every vulnerability which aids security personnel to keep track and address specific vulnerabilities.

3. Contracts with vendors must include security requirements and right-to-audit clauses. The security procedures are all requirements because they are fundamental and needed to maintain a high level of security. The right-to-audit clauses are needed to ensure that these vendors and third parties are in compliance at all times.

5.9 Policy Enforcement

1. Compliance with this policy will be measured through audits, reviews, and automated scans. Internal reviews and reviews for third-parties will be done on a regular cycle/basis to ensure total compliance with the policy.

2. Non-compliance may result in disciplinary action for employees or termination of contracts for vendors. Depending on the vastness and the level of non-compliance or contract breaking will determine whether or not further legal action would need to be taken against those who do these actions.

3. exceptions to the policy must be documented, justified, and approved by the Security Governance Board. This ensures that there is pre-determined information that is available for all to know who has these exceptions and what exceptions they have.

5.10 Policy Review

1. The policy will be reviewed annually or after significant changes in:

   (a) Technology stack (changes towards microservices, new frameworks)

   (b) Legal requirements (new data protection laws or regulations)

   (c) Business strategy or changes (entering new markets or getting into deals with new groups that have different compliance needs)

2. Updates will be communicated through internal briefings, documentation, and training sessions. Ensuring that there are high levels of communication so there will be no errors or faults in any level.

Chapter 6

Software Compliance

6.1 Purpose

The purpose of this policy is to ensure all Honda Group entities maintain full compliance with software licensing agreements, copyright laws, and internal software usage guidelines. This policy helps reduce legal and financial risks, promotes cybersecurity hygiene, and upholds Honda's commitment to ethical and lawful business practices.

6.2 Scope

This policy applies to:

All Honda employees, contractors, and vendors with access to Honda-owned systems.

All software used on Honda devices (desktops, laptops, servers, mobile devices, embedded systems, etc.).

All Honda business units, including R&D, manufacturing, sales, marketing, logistics, and administration.

On-premises and cloud-based software, open-source components, and SaaS platforms.

6.3 Policy Statement

Honda strictly prohibits the use of unlicensed, unauthorized, or pirated software. All software installations and use must be pre-approved, centrally managed, and tracked by the IT department or designated software asset management (SAM) teams. Violations of this policy may result in disciplinary action, up to and including termination or legal prosecution.

6.4 Software Usage Requirements

Procurement: All software must be acquired through approved procurement channels. No employee may download, install, or purchase software independently for work use.

Licensing: All software must be properly licensed. Proof of purchase, license keys, or contracts must be maintained for audit purposes.

Installation: Only authorized IT personnel may install software on Honda devices unless approved self-service portals are available.

Open-Source Software (OSS): OSS will be used only if:

It is approved by the IT Governance team.

Its licensing terms (e.g., GPL, MIT, Apache) are compatible with Honda's intended use.

It does not introduce legal, operational, or security risks.

Cloud and SaaS Applications: Usage of SaaS tools must be reviewed for data protection, compliance (e.g., GDPR, CCPA), and contractual obligations.

Prohibited Software:

Pirated, cracked, or unauthorized software.

Software used for cryptocurrency mining.

Personal-use entertainment or file-sharing apps (unless explicitly approved.

6.5 Roles and Responsibilities

Executive Leadership Provide funding and strategic support for software asset compliance.

IT Governance and Compliance Enforce the policy, conduct audits, and manage the software inventory. Maintain a software license register and ensure contractual compliance.

Business Units Request approved software via official channels. Report non-compliant software or licensing concerns.

Employees Use only approved and licensed software. Refrain from altering or bypassing license restrictions. Promptly report suspected software misuse.

6.6 Software Asset Management (Sam)

Honda will implement a formal SAM program, which includes:

Centralized inventory of all software assets. Periodic audits to detect unlicensed or unused software. Lifecycle management (procurement to retirement). Vendor contract review and license renewal tracking.

6.7 Monitor and Auditing

Honda reserves the right to monitor devices for unauthorized software.

Internal audits will be performed annually or as needed.

Third-party audits will be conducted to ensure regulatory and contractual compliance.

6.8 Violation and Disciplinary Action

Any employee discovered using unauthorized software or violating licensing terms will face disciplinary action, which will include:

Formal warnings Removal of system access Termination of employment Legal action or liability for damages

6.9 Exceptions

Requests for exception must be formally submitted to the IT Governance & Compliance team, accompanied by business justification and risk assessment. Approved exceptions will be documented and reviewed annually.

6.10 Policy Review and Maintenance

This policy will be reviewed annually by the Global IT Governance & Compliance team or upon significant software-related incidents or regulatory changes.

Chapter 7

Bring Your Own Device (BYOD)

7.1 Purpose

To provide flexibility to its associates, Honda permits the use of personal computers and mobile devices ("Personal Devices") to access certain Honda resources, provided they meet strict security requirements. This policy defines the requirements and responsibilities for any associate who wants to participate in the BYOD program. The goal of this policy is to protect Honda's systems and date while providing associates with the convenience of utilizing their personal devices. Participation in the BYOD program is voluntary and constitutes acceptance of the terms herein.

7.2 Scope

This policy applies to all authorized users (Honda associates, contractors, and other authorized personnel) who wish to use a personal smartphone, tablet, laptop, or desktop computer to access Honda email, applications, or data.

7.3 Device Eligibility and Registration

1. **Supported Devices:** Only devices with modern, actively supported operating systems (e.g., iOS, Android, Windows, macOS) are eligible. Devices that are "jailbroken", "rooted", or have had their operating system security controls disabled are forbidden.
2. **Registration:** All personal devices must be registered with Honda's IT department through the approved Mobile Device Management (MDM) or security portal before being used to access any Honda resources.

7.4 Minimum Security Requirements

To be granted access, all personal devices must comply with the following:

1. **Strong Password/Biometrics:** The device must be secured with a strong password as defined in the password policy or an approved biometric control.
2. **Encryption:** Storage spaces containing Honda data must be encrypted.
3. **Honda Security Software:** Users must consent to the installation of Honda-mandated security software such as an MDM profile or an endpoint security agent. This software provides Honda with the ability to enforce security policies and protect corporate data.
4. **Updated Software:** The operating system and all applications must be kept up to date with the latest security patches.
5. **Unapproved Software:** Devices containing software that is untrusted or designed to circumvent security controls are forbidden.

6. **Malware Protection:** Device must have a clean scan from Honda antivirus software weekly to remain eligible.

7.5 Acceptable Use

1. **Data Segregation:** Honda data must be stored, accessed, and managed exclusively within Honda-approved applications and secure containers provided by the MDM. Storing Honda data in personal applications, personal cloud storage, or on the device's local file system outside the secure container is strictly forbidden.
2. **Camera and Microphone Use:** Users must not use the device's camera, microphone, or screen recording features to capture or transmit confidential Honda information without explicit authorization.
3. **Personal Use:** While the device is personally owned, users must not engage in illegal, or policy violating activities while using the device to access company resources. Honda is not responsible for any costs associated with personal use (e.g., data plans, maintenance).

7.6 Honda's Rights and Responsibilities

By participating in the BYOD program, users acknowledge and agree that Honda has the right to:

1. **Monitor Compliance:** Audit the device to ensure it complies with this policy.
2. **Enforce Policies:** Push security configurations to the device, such as Wi-Fi settings, password requirements, and application restrictions.
3. **Wipe Corporate Data:** Selectively wipe all Honda data and remove Honda applications from the device. This action will be performed if the device is lost, stolen, found to be non-compliant, or upon the user's separation from Honda. This process is designed to leave personal data untouched.
4. **Full Device Wipe:** In extreme cases where a device is lost or stolen and poses a significant risk to Honda, a full factory reset of the device may be initiated. Honda is not liable for the loss of personal data in such an event.

7.7 User Responsibilities

1. **Reporting:** Users must immediately report a lost or stolen device to the Honda Help Desk.
2. **Maintenance:** Users are responsible for the maintenance, repair, and data plans for their personal devices.
3. **Backups:** Users are solely responsible for backing up their personal data. Honda is not responsible for any loss of personal photos, documents, or other information.

7.8 Policy Enforcement

Non-compliance with this policy may lead to the revocation of BYOD privileges and disciplinary action, up to and including termination of employment or contract.

Chapter 8

Clean Desk Policy

8.1 Purpose

The purpose of this Clean Desk Policy is to protect sensitive information and maintain a secure, organized, and professional work environment by ensuring that all workspaces are kept clear of confidential materials when not in use.

8.2 Scope

This policy applies to all employees, contractors, interns, and temporary staff who work in or access the organization's facilities, whether on-site or remote. Any exceptions to this policy must be approved by the Information Security Officer (ISO) or a designated authority.

8.3 Policy Guidelines

General Requirements

1. At the end of each workday, all workspaces must be cleared of sensitive or confidential information.
2. Workstations must remain tidy and organized during the day to reduce the risk of unauthorized access.

Physical Documents

1. All confidential documents must be stored in a locked drawer, cabinet, or secure storage area when not in use.
2. Documents containing personally identifiable information (PII), financial data, proprietary business information, or customer data must never be left unattended.
3. Shred or securely dispose of documents when they are no longer needed.

Electronic Devices

1. Lock computer screens when leaving the desk, even for short periods.
2. Log off or shut down systems at the end of the workday.
3. Laptops and other portable devices must be secured in a locked drawer or cabinet when not in use.

Removable Media

1. USB drives, external hard drives, and other removable media must be stored securely and clearly labeled.
2. Remove all removable media from computers and lock them away when not in use.

Whiteboards and Notes

1. Erase whiteboards that contain sensitive information at the end of meetings or the workday.
2. Do not leave handwritten notes, sticky notes, or passwords exposed on desks, monitors, or keyboards.

8.4 Remote Work Considerations

1. Remote workers must apply the same clean desk standards in their home or remote work environments.
2. Confidential materials must be stored securely, and screens should be locked when unattended.

8.5 Compliance and Enforcement

Violations may result in disciplinary action, up to and including termination. Random audits may be conducted to ensure compliance with this policy.

Chapter 9

Email Security Policy

9.1 Purpose

The purpose of this policy is to define the proper use of email and Internet services for Honda. These guidelines are designed to protect sensitive company information, reduce the risk of cyber security threats, and maintain compliance with both corporate and legal standards. All users of HMIN's digital communication systems must adhere to the rules described in this policy.

9.2 Scope

This policy applies to all individuals with access to Honda's email or internet systems, including full-time associates, part-time workers, contractors, interns, and third-party service providers. All users are to follow these rules regardless of job role or location within the facility.

9.3 Email Use

1. Email systems at Honda are provided exclusively for business-related communication. Personal use of email accounts is prohibited. Users must not send or forward confidential or proprietary information without proper authorization, and any sensitive data transmitted via email must be encrypted.
2. It is critical to remain cautious of phishing emails; users should not click on suspicious links or open unknown attachments, and any questionable messages must be reported to the IT Helpdesk immediately.
3. Automatic forwarding of emails to non-Honda email accounts is strictly forbidden unless explicitly approved by IT Security.
4. Sending or receiving offensive, harassing, or inappropriate content through the company email system will not be tolerated and may result in disciplinary action.

9.4 Web Access

1. Internet access at Honda is provided to support business productivity, research, and communication. Limited personal use may be allowed during designated breaks as long as it does not disrupt workflow or compromise network security.
2. Accessing websites that host adult content, gambling platforms, hate speech, or illegal material is strictly prohibited.
3. Social media use is restricted to official business communications and requires prior approval from the Communications or HR departments.

9.5 Monitoring and Environment

All use of email and web services is subject to monitoring by the Honda IT Security team. Activities will be logged to ensure compliance with this policy and to investigate any suspected violations. Users have no expectation of privacy when using company-provided digital tools. Violations of this policy may result in disciplinary actions ranging from a warning to termination of employment, and may include legal consequences depending on the nature of the offense.

9.6 Enforcement

Violations of this policy may result in disciplinary actions ranging from a warning to termination of employment, and may include legal consequences depending on the nature of the offense.

Chapter 10

Third-Party Security Policy

10.1 Purpose

Honda's third party Security Policy exists to protect the company's digital infrastructure, confidential data, and customer privacy. This policy is mandatory for all third party entities that engage in any form of business with Honda. This includes, but is not limited to, contractors, software vendors, service providers, IT partners, logistics providers, and manufacturers. All third party companies must sign and adhere to the policy before beginning any operations with Honda. There are no exceptions. Any third party that fails to meet these requirements will be denied access to Honda's systems and will be disqualified from further business.This policy outlines exact rules and standards that must be followed at all times when handling, storing, accessing, or transmitting Honda's digital assets or physical components connected to Honda's IT or production systems. All personnel within a third party organization are required to comply. Honda holds the vendor fully accountable for any violations committed by its employees.

10.2 Scope

This policy outlines exact rules and standards that must be followed at all times when handling, storing, accessing, or transmitting Honda's digital assets or physical components connected to Honda's IT or production systems. All personnel within a third party organization are required to comply. Honda holds the vendor fully accountable for any violations committed by its employees.

10.3 Core Security Requirements

1. All Honda related data must be treated as confidential and must be encrypted during transmission and while stored. Third parties will not copy, share, or store Honda's data without written permission. Any attempt to move, replicate, or disclose Honda data to unauthorized parties is strictly prohibited.

2. System access is limited to authorized personnel only. Third party organizations must implement strict identity verification, including multi-factor authentication. Passwords must meet Honda's complexity standards and must be changed regularly. Shared accounts are forbidden. Access logs must be kept and made available to Honda on request.

3. Any Third-Party device connected to Honda's systems or networks must be secured with up to date antivirus, firewalls, and intrusion detection tools. Personal or unauthorized devices are not permitted under any circumstance. All remote access connections must pass security approval and must use a secure VPN with logging enabled.

4. All third party staff with access to Honda data or systems must complete formal cybersecurity training. This training must be renewed annually and must cover phishing, malware, password protection, and data handling policies. Records of completed training must be provided to Honda on request.

5. Any suspected or confirmed security incident, breach, or threat must be reported to Honda's Information Security team within 24 hours. Failure to report an incident on time will result in immediate review, suspension of access, and potential termination of the relationship.

6. There is no flexibility in Honda's third party Security Policy. Every rule must be followed, every system must be protected, and every person involved must be trained. Any company unwilling or unable to meet these standards will be removed from Honda's partner network. Security is not optional, it is a requirement.

10.4 Monitoring and Audits

Honda will perform both scheduled and non-scheduled audits to verify that third party partners are following all aspects of the security policy. These audits will include system checks, documentation reviews, interviews, and physical inspections if applicable. Honda requires quarterly compliance reports from all critical third parties. These reports must include, System access logs, Encryption practices, Patch/update schedules, Incident response testing results, and Security training records.

10.5 Enforcement

Honda's third party security policy is a legal agreement. Any company that violates the terms of this policy will face penalties, including, Termination of contract, Legal action for damages, Public disclosure of the incident, Government fines If a third party's failure leads to a data breach, they will be held liable for all costs related to the breach, including technical investigations, customer notifications, recovery, legal fees, and reputation management.

Chapter 11

Server Security

11.1 Purpose

The purpose of this policy is to define the minimum security controls required to ensure the confidentiality, integrity, and availability (CIA Triad) of the company's server infrastructure in regards to the Greensburg, Indiana Honda facility. Simultaneously the purpose of this policy is to mitigate the risk of unauthorized access, data breaches, malware propagation, operational disruptions, and other cyber-threats that could affect all areas of business continuity along with intellectual property, safety systems, or regulatory compliance.

11.2 Scope

The server security applies to all physical and virtual servers, both company owned or third-party managed, that do any of the following processes: Store, process, or transmit sensitive company data or information otherwise associated with performing critical business functions. the following are subject to the server security policy:

1. **Deployment Scope:** Physical servers, virtual machines, cloud based instances, containerized services, and edge computing systems
2. **Functional Scope:** Domain Controllers, Database servers, Web and application servers, Log aggregation servers, CI/CD servers, License servers, and email or collaboration servers
3. **Personnel and access scope:** the policy and its guidelines apply to system administrators, developers, DevOps/DevSecOps personnel, cloud engineers, and third-party vendors. All personnel responsible for deploying, configuring, or accessing security controls for company servers.
4. **Life Cycle Scope:** The server security policy governs all phases of server development. this includes procurement, configuration, hardening, patching, monitoring, backup and disaster recovery, incident response integration, and finally decommissioning and data destruction

This policy applies to all server infrastructure housed within the Greensburg, Indiana Honda facility. The policy also extends to cloud-based workloads and hybrid deployments that interconnect with or impact the security posture of the company's global server ecosystem. Regional variations in regulatory or data residency requirements must be accounted for during implementation.

11.3 Server Configuration

All servers must be deployed using pre-approved, hardened images or templates aligned with CIS benchmarks or NIST 800-53 standards. The goal is to minimize attack surface and ensure secure, consistent configurations across all environments.

1. **Baseline and Deployment:** Company servers must utilize golden images that only include required services, security agents, and configuration management tools. All unnecessary services, tools, packages must be disabled or removed before a server can be deployed. all deployed server

hardware or software must comply with the following standards: ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework (CSF), CIS Controls, NIST SP 800-53, NIST SP 800-171, FedRAMP, FISMA, HIPAA (if applicable), and PCI DSS.

2. **OS and Network Hardening:** Operating systems must be patched regularly. Patches considered to be mission critical are to be implemented within a reasonable time frame. Local firewalls must be enabled at all times with restrictive and explicit rule sets. Any and all remote access points must utilize encryption along with multi-factor authentication. Root/Admin accounts must be disabled for direct login; access granted through privileged access management tools or jump hosts.

3. **Credential Security:** All users must authenticate with unique accounts and be assigned minimum required privileges. Service accounts must be non-interactive along with credentials rotated automatically. Users must consult company password policy when creating user accounts and passwords.

4. **Logging and Monitoring:** All forms of system logs must be enabled and forwarded to a centralized Security Information and Event Management device (SIEM) within 60 seconds. Logs must capture authentication events, privilege escalations, system changes, and software installs. file integrity monitoring is to be enabled on sensitive or high priority directories

5. **Host-Level Protections:** All servers must run company standard endpoint security. Memory protections must be enabled where supported. vulnerability scanners must run at least monthly, with remediation tracked and enforced.

6. **Change Control and Configuration Drift:** All servers changes must be made through company approved configuration management systems. Drift detection tools must be in place and used to detect unauthorized or out-of-policy changes.

11.4 Physical Server Security

To protect against unauthorized physical access, damage, or interference, all servers must meet our security requirements to be housed within onsite locations. Physical severs located on premises must adhere to the following requirements.

1. **Restricted Access:** Server rooms must be accessible only to authorized personnel. Authorized personnel must utilize two of the following access control systems: key cards, biometric scanners, or security codes. These security controls shall be implemented and reviewed regularly at any site where servers or related hardware is housed.

2. **Environmental Controls:** Environmental Controls: Server environments must maintain stable temperature and humidity levels using appropriate HVAC systems. Fire suppression, smoke detection, and water leak detection systems must be in place and tested regularly.

3. **Surveillance and Monitoring:** Physical access points to the server room must be monitored at all times when possible with surveillance cameras (CCTV). Logs of physical access shall be maintained and reviewed periodically.

4. **Visitor Management:** All visitors must be signed in, escorted at all times, and recorded in an access log. No unauthorized equipment may be brought into or removed from the server room without prior approval.

5. **Locking Mechanisms:** All server racks must be locked when not in active maintenance. Portable storage devices must not be left unattended in the server area.

6. **Power Protection:** Servers must be connected to uninterruptible power supplies (UPS) and backup generators to ensure continuous operation during power outages.

7. **Asset Inventory:** All physical servers and related equipment must be documented in an asset inventory, including serial numbers, location, and assigned custodian.

These controls ensure the confidentiality, integrity, and availability of systems by reducing risks associated with physical threats and unauthorized access.

11.5 Vulnerability Management

Vulnerability management ensures timely identification, assessment, and remediation of security flaws across all server environments. All systems must be regularly scanned using company approved tools, with findings prioritized based on common vulnerability scoring system (CVSS) scores, exploit availability, data sensitivity, and operational impact. Remediation must follow the predefined guidelines of a service level agreement (SLA), be verified through re scanning, and are cohesive with change management procedures. Key performance indicators such as patch compliance, time-to-remediate, and exception tracking must be reported to Security Governance on a monthly basis.

1. **Risk Based Prioritization:** All identified Vulnerabilities must be ranked based on CVSS score, exploit availability, asset sensitivity, and operational impact. Vulnerabilities with the highest scores will receive top remediation priority
2. **Remediation and Validation Policy:** Patches or mitigation actions must be applied within defined SLA timelines. All remediated systems must undergo vetting and verification through scanning to confirm vulnerability resolution.

11.6 Server Decommissioning

Prior to decommission, all data stored or otherwise cached in a server must be securely wiped or destroyed following NIST 800-88 standards. A formal decommissioning checklist with documentation must be completed and signed off by the appropriate IT authority. Decommissioned hardware must be inventoried or destroyed, or returned to vendors per contractual terms.

11.7 Third-Party Servers

Third-Party access to company servers must be governed by a legally binding document, such as an NDA, along with a data-sharing agreement. Required stipulations for the NDA and data sharing agreement are as follows: Vendors may only access resources necessary for required contract fulfillment. Permanent data storage by external parties is prohibited unless explicitly authorized by the legal department and the appropriate information security authority.

11.8 Enforcement

Violations of the server security policy may result in disciplinary action, including termination of access, employee disciplinary measures, or legal action. All incidents will be reviewed by legal departments.

11.9 Exceptions

All exceptions must be reviewed and approved in writing by the appropriate IT or security authority and documented with appropriate risk analysis.

Chapter 12

Remote Access

12.1 Purpose

The purpose of this policy is to define rules and requirements for connecting to Honda's network from any host. These rules and requirements are designed to minimize the potential exposure to Honda from damages which may result from unauthorized use of Honda's resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

12.2 Scope

This policy applies to all Honda employees, contractors, vendors and agents (hereafter referred to as "Users") using Honda-owned, or personal devices (refer to BYOD policy for applicable devices) to connect to Honda's internal network, systems, or data from offsite. This policy applies to remote access connections used to do work on behalf of Honda, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Honda networks.

12.3 Device Requirements

All devices used for remote access, whether Honda-owned or personal, must meet the security standards defined by Honda.

1. **Company-Issued Devices:** Preconfigured by Honda's IT to meet all security requirements
2. **BYOD devices:** Must be fully compliant with all requirements outlined in the Honda BYOD Policy before being granted remote access.

12.4 Approved Access Method and Authentication

1. **VPN Required:** All remote connections to the Honda internal network must be made through the company-approved Virtual Private Network (VPN) client. Any other method is forbidden unless explicitly granted in writing by the IT Security Department.
2. **No Split-Tunneling:** Split-tunneling is strictly prohibited. All network traffic from the remote device must be routed through Honda's security infrastructure while the VPN is active.
3. **Multi-Factor Authentication (MFA):** All remote access attempts must be authenticated using a Honda-approved MFA solution.

12.5 Secure Connection Environment

Users are responsible for ensuring their connection is secure. The use of public, untrusted, or unsecured Wi-Fi networks (e.g., at cafes, airports, hotels) for remote access is strictly prohibited. Connections should only be made from trusted networks, such as a secure home office network.

12.6 Data Handling

1. **Prohibition of Local Storage:** Storing Honda's confidential, secret, or restricted data on a local drive of a remote device is strictly prohibited. All work must be saved directly to approved network or cloud locations (e.g., network drives, SharePoint).
2. **Physical Security:** Users are responsible for the physical security of their devices. Devices must not be left unattended in public, and the use of privacy screens is strongly encouraged.

12.7 Session Management

1. **Idle Timeout:** Remote VPN sessions will be automatically disconnected after 30 minutes of inactivity. Users must re-authenticate to resume the session.
2. **Lock Screen:** Users must lock their device screen whenever they step away from it.
3. **Log Off:** Users must fully log off from the VPN and all corporate applications at the end of their workday.

12.8 Roles and Responsibilities

1. **Users:** Responsible for understanding and adhering to this policy and the BYOD policy if applicable.
2. **IT Department:** Responsible for managing and securing the remote access infrastructure (VPN, MFA).
3. **Information Security Team:** Responsible for defining security standards, monitoring for compliance, and updating this policy.
4. **Management:** Responsible for ensuring their team members are aware of and comply with this policy.

12.9 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

12.10 Policy Enforcement and Compliance

Failure to comply with this policy may result in the immediate revocation of remote access privileges and further disciplinary action, up to and including termination of employment or contract. Honda reserves the right to audit remote connections to ensure compliance.

Chapter 13

Encryption Policy

13.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States. The purpose of this document is also to protect customer data and to ensure confidentiality with all of Honda's sensitive data.

13.2 Scope

This policy's applies to all Honda employees and affiliates.

13.3 Safeguards

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "par- tially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Tech- nology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption. These safeguards ensure to keep customer privacy confidential. All sensitive vehicle data such as Telematics and CAN should be encrypted using authenticated encryption (AES-GCM) to prevent replay at- tacks in accordance with honda's vehicle security standards. Telematics is a system in which a vehicle sends and recives data and is used for GPS tracking. Telematics ensures that vehicles can communicate with external systems. All Third party partners are required to adhere to these security standards. To protect data stored on any virtual and physical media sensitive data should use industry standard algorithms such as AES-256 and Encryption must be applies to all servers, databases, cloud storage, and vehicle storage systems. To Ensure accessibility encrypted data must be backed up weekly, every Monday at 2:00am est

- Use only AES-compatible or FIPS 140-2 approved encryption algorithms
- AES is recommended for symmetric encryption and RSA and ECC for asymmetric.
- Vehicle data such as Telematics, CAN must use AES-GCM to prevent replay attacks.
- Third parties must follow Honda's encryption standards.
- Servers, Databases, Cloud, Vehicle Systems must use AES-256 encryption.
- All encrypted Data must be backed up weekly, Monday at 2:00 AM EST

13.4 Policy sanctions

Non-compliance may result in severe cases may result in disciplinary conse- quences such as termination of employment or legal conseqences. In less severe consequences a formal warning or mandatory retraining will be enforced. Ac- cessing unauthorized data or system compromise will be reported to agencies such as NHTSA, FTC or GDPR. For Third-parties failure to comply may result in immediate suspension, financial penalties, and reporting to legal authorities.

1. Non-compliance may result in severe cases may result in disciplinary conse- quences such as termination of employment or legal conseqences.
2. In less severe consequences a formal warning or mandatory retraining will be enforced.
3. Ac- cessing unauthorized data or system compromise will be reported to agencies such as NHTSA, FTC or GDPR. For Third-parties failure to comply may result in immediate suspension, financial penalties, and reporting to legal authorities.

Chapter 14

Firewall Policy

14.1 Purpose

This policy is established to both secure and protect the digital infrastructure of Honda. from potential cybersecurity threats by regulating the deployment, configuration, and use of firewalls. The goal is to protect the organization's sensitive information and information systems' confidentiality, integrity, and availability. The firewall is a critical component of our network security infrastructure and is designed to:

1. Allow secure remote access via virtual private networks (VPNs).
2. Control access to the internal trusted network and the external untrusted network.
3. Ensure strong and updated authentication for all technological systems that can be exploited.
4. Keep insecure internal systems hidden and protected from the internet.
5. Monitor every traffic entering and departing the internal network.
6. Maintain the privacy of critical information and prevent unauthorized access to intellectual property.
7. Stop network traffic that could be harmful or unwanted.

14.2 Scope

This policy applies to all employees, contractors, and third-party entities who have access to the network, information systems, and linked devices of Honda. This includes, but is not limited to, departments, business units, and any persons responsible for network firewall configuration and maintenance. The policy applies to all firewalls and related components, regardless of where they are located or who owns them. Firewall security is a shared responsibility involving several key roles within Honda. Each role is critical to the protection of network infrastructure, systems, and data against cyber threats.

14.3 Policies and Procedures

All firewalls employed by Honda must adhere to security requirements and industry best practices. Access, traffic rules, configuration details, and filtering methods must be documented and periodically reviewed to ensure effectiveness and currency. Annual testing of Honda's firewall is integral to our overall security program. The testing process ensures that the firewall functions as intended and provides the required level of protection for our network and systems.

14.4 Access Control

Access to firewall systems must be governed by strict access control measures to ensure that only authorized personnel can view, modify, or manage firewall configurations. Role-based access control (RBAC)

must be enforced, with permissions granted based on the job function and need-to-know. Any exceptions must be approved by management (for more information consult section 14.15 Request for Change and Exceptions).

14.5 Traffic Rules

Firewall traffic rules govern what types of traffic are allowed to enter, exit, or move within the company's network. These rules must follow the principles of least privileged, default deny, and any and all industry standard practices. Permitting only traffic that is explicitly authorized and necessary for business operations.

14.6 Filtering Methods

Firewall filtering methods must follow best practices and apply the principles of least privilege and default deny to restrict access to only authorized and necessary services. Filtering methods will require using anomaly detection and all anomalies detected will be logged and may be used to generate temporary firewall rules. Annual assessments will be conducted to ensure consistent and up to date firewall filtering methods.

14.7 Firewall Configuration Guidelines

Firewall configurations must be implemented using secure baselines, documented standards, and change management procedures to minimize vulnerabilities and maintain operational integrity.

14.8 Firewall Testing Guidelines

Firewall systems must undergo quarterly testing to verify proper functionality, identify vulnerabilities, and ensure that security controls are operating as intended. Testing must be performed using structured methodologies, such as vulnerability scanning, rule validation, and penetration testing, in accordance with the company's security standards.

14.9 Compliance

Honda is committed to adhering to all applicable cybersecurity and privacy requirements. Annual audits, assessments, and upgrades are performed to ensure compliance with industry standards and regulatory obligations. To uphold this commitment Honda will:

1. Regular audits and assessments are conducted to verify adherence to the company's firewall policy and relevant frameworks such as ISO/SAE 21434, ISO/IEC 27001, NIST SP 800-82, GDPR, and other applicable international, federal, and local regulations.

2. Firewall configurations and rule sets are reviewed and updated in accordance with industry best practices, evolving threats, and compliance mandates. Firewalls must be patched and up to date to maintain a strong security posture.

3. Documentation and change records related to firewall management are maintained for audit readiness and transparency.

4. Training and awareness initiatives are conducted to ensure employees and administrators understand their roles in maintaining compliance. For more information consult Chapter 4 Security Awareness.

14.10 Firewall Documentation Guidelines

Honda's firewalls require thorough and detailed documentation, ensuring quarterly accessibility updates. For transparency, document changes with reasons, accountable parties, and timestamps. Create precise diagrams emphasizing firewall location for efficient communication. Create standard operating procedures for revisions, testing, monitoring, and responding to incidents. Commit quarterly audits to documentation to ensure its accuracy and relevance. Utilize real-time platforms to create comprehensive and shareable documentation. Follow predefined retention periods that are in accordance with industry norms and legal obligation. Conduct annual training to raise awareness and comprehension of the value of documentation.

14.11 Revision and Update Process

1. Updates to the policy will be made based on:
   (a) Risk assessments and audit findings.
   (b) Advances in firewall technology and best practices.
   (c) Feedback from internal and external stakeholders.
   (d) Emerging cybersecurity threats or vulnerabilities.

1. All policy revisions must be:
   (a) Documented with version control.
   (b) Reviewed and approved by the Chief Information Security Officer (CISO).
   (c) Communicated to all relevant personnel and departments.

14.12 Training and Communication

1. After each policy revision, targeted training sessions will be provided to affected teams to ensure understanding and proper implementation.
2. Stakeholders will be notified of the changes through appropriate internal communication channels.

14.13 Request for Change and Exceptions

Honda, has established a due process for managing requests for change and exceptions to firewall policies. This allows authorized personnel to submit requests for specific services not permitted by default. The change and exceptions require permission from the designated authorities in accordance with the security guidelines set by Honda.

14.14 Violations

Violations of the firewall policy of Honda. are considered serious breaches of corporate security protocols and may result in disciplinary action, up to and including termination of employment, revocation of system access, or legal consequences, depending on the nature and severity of the offense. Examples of Violations Include (but are not limited to):

1. Attempting to bypass or circumvent firewall protections or access restrictions.
2. Making unauthorized modifications to firewall configurations, rules, or access controls.
3. Disabling, deactivating, or tampering with firewall systems without proper authorization.
4. Sharing credentials or access permissions used to manage or bypass firewall systems.
5. Failing to report known or suspected policy violations, misconfigurations, or suspicious activity.

6. Sharing credentials or access permissions used to manage or bypass firewall systems. At no time should any Honda employee, contractors or third-party partners ask for your credentials. If asked for your credentials, immediately report it to a member of management, IT department, or IT security team.

Chapter 15

Network Diagram

15.1 Purpose

The purpose of the Network Diagram section is to establish clear guidelines and requirements for the creation, maintenance, and protection network diagram information/infrastructure. Accurate network diagrams are critical to understanding our site's IT infrastructure, facilitating trouble shooting, maintenance, information relevant to incident response, and validating compliance with security standards and regulations. Following the guidelines of this policy ensures that all network diagrams accurately represent the current state of Honda Motor Co., Ltd. Greensburg Indiana Site, including all operation critical systems, devices, communication links, and security boundaries. Not only this but this policy defines how these diagrams must be classified, stored, and shared to prevent unauthorized access and protect sensitive information. By enforcing a structured and secure approach to diagram management, the organization reduces the risk of threats, enhances incident recovery efficiency, and supports ongoing network audits and compliance efforts.

15.2 Scope

The policies regarding the network diagram are subject to any/all persons or groups that have access to the network diagram and infrastructure data. This includes network and system administrators, IT staff, contractors, and third-party vendors who design, modify, or manage network infrastructure within the Greensburg, Indiana Honda facility.

15.3 Policy requirements

This section highlights the mandatory requirements for the creation, classification, maintenance, and use of network diagrams throughout Honda Motor Co., Ltd.

1. **Accuracy and completeness:** All network diagrams and associated network infrastructure documentation are required to reflect the state of logical and physical network topologies according to the date it is recorded or created.

2. **Key components:** Network diagrams must include business standard nomenclature along with accurate labeling. Diagrams are obligated to label key infrastructure components.

3. **Operational Technology and Diagram crossover:** OT environments must be diagrammed separately from network infrastructure but still integrated at crossover points (e.g., firewalls or data aggregators)

4. **Diagram discrepancies:** Network diagrams must be updated when modifications to the network occur. When a change is instituted, network diagrams must be dated when last modified. In the event that an individual finds an incomplete, outdated, or inconsistent network diagram, the procedure is to report the discrepancies to a supervisor or administrator.

5. **Standardization and format:** All diagrams must adhere to standardized format and notation. All diagramming tools must be company-approved. Diagrams must include accurate dates, version numbers, authors, legends, appropriate labels for zones and devices. Standardized format is required to ensure that diagrams are universally understandable across teams and departments.

6. **Classification and access control:** All network diagrams mapping Honda Motor Co., Ltd. sites are confidential information. Informational security is critical to reducing risk. All network diagrams and associated infrastructure documentation must be stored in secure document repositories. Security controls that are to be used to control access are role-based access controls, multi-factor authentication, along with encrypted storage and transmission. Access logs must be maintained for all diagrams representing critical infrastructure

7. **Version Control and Change management** All network diagrams must include history with timestamps, authors, and edit descriptions. In the event of modification to network resources the appropriate editor must update the network within a reasonable time frame. Any and all modifications to the network diagram must approved by the appropriate authority as well as vetted by company change control processes.

8. **Storage, backup and retention** Network diagrams are subject to the Honda Motor Co., Ltd. backup policy and must be included in regular backup cycles alongside other mission-critical information assets. Network Diagrams must be retained for at least as long required by regulation or audit standards. Accurate offline backups must exist for network diagrams at all sites to ensure availability during network outages, cyber incidents, or loss of primary access systems.

9. **Incident response and emergency access** Network diagrams must be integrated into Honda Motor Co., Ltd. Incident Response Plan (IRP). Emergency versions must adhere to the following guidelines. Diagrams must be stored in designated security operations centers (SOCs), reasonably accessible during a declared cyber event or outage, available in both digital and physical form for high priority sites.

10. **Review and audit** Network diagrams must adhere to the guidelines regarding accuracy validation. Diagrams must be certified as accurate as soon as possible after any infrastructure project or re-architecture, or after revalidation of network diagram discrepancies

15.4 Third-Party access and sharing of network diagrams

To preserve the confidentiality and integrity of Honda Motor Co., Ltd. network architecture, third-party access to network diagrams is strictly regulated. Due to the fact network diagrams may expose sensitive system configurations, segmentation zones, and security controls or other, any access granted to external entities must be carefully controlled and limited to only that which is strictly necessary. Prior to sharing any network diagrams with third-party entities, service providers, auditors, consultants, or other, the following requirements must be met:

1. **Non-disclosure agreement (NDA):** A legally binding and current NDA must be in place between Honda Motor Co., Ltd. and the third party. The NDA must cover the handling of network infrastructure and sensitive documentation.

2. **Data sharing agreement:** A data-sharing agreement must be vetted and approved by both by the legal department and information security office. this agreement must define the scope, duration, purpose, and the handling requirements for all information and documentation regarding network diagrams and infrastructure.

3. **Role-based and scope limitations:** Third-party access is limited to individuals whose job responsibilities necessitate direct interaction with the applicable network segment(s). Blanket access is not permitted. Shared diagrams must be limited to include only the relevant portions necessary for the third party to perform its contracted duties.

4. **Handling and Security obligations:** All network diagrams must be communicated through secure and encrypted channels. All communicated network diagrams must be watermarked and labeled appropriately according to its classification. Third parties are not permitted to alter, replicate, or redistribute the diagrams without prior written authorization from Honda Motor Co.,

Ltd. Access is restricted by time, and credentials must be revoked immediately upon completion of the contractual agreement or upon termination of the agreement.

5. **Third-party long term retention:** Third parties are strictly prohibited from retaining permanent copies of any network diagram unless it meets the following expectations. It is explicitly required as part of the contractual engagement and written approval has been granted by the Information Security Office and Legal Department. In all other cases all copies must be returned or securely destroyed at the conclusion of the agreement, and the third party must provide documented proof of destruction upon request.

6. **Compliance and audit:** Third-party access to network diagrams is subject to audit by Honda Motor Co., Ltd. at any time during or after the terms of the agreement. Any violations of these terms may result in immediate termination of access, contract cancellation, and/or legal action.

15.5 Enforcement

Violations of this policy may result in disciplinary action, including access revocation, reassignment, formal reprimand, or termination of contract. In cases where violations result in regulatory non-compliance or security breaches, offenders may be reported to the appropriate internal governance bodies and/or regulatory authorities.

15.6 Network Diagram

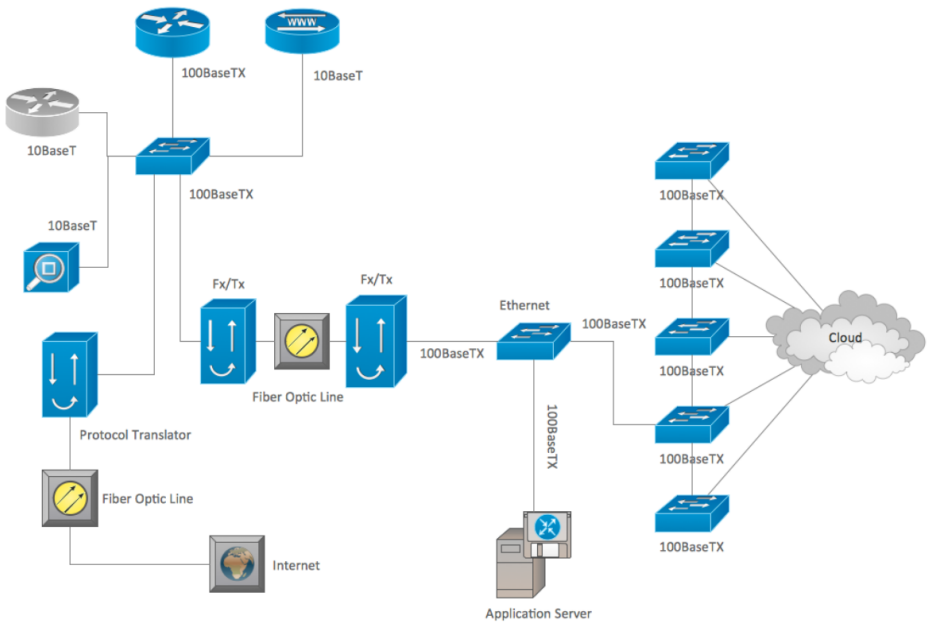

Figure 15.1: Representation similar to our company network

Chapter 16

Disaster Recovery Policy

16.1 Purpose

The purpose of this Disaster Recovery (DR) Policy is to establish a structured approach for Honda to prepare for, respond to, and recover from disruptive events that impact business operations, IT infrastructure, or production lines. This policy ensures the continuity of mission-critical services and protects employees, customers, assets, and reputation.

16.2 Scope

This policy applies to:

All Honda Group business units (e.g., Honda Motor Co., American Honda, Honda R&D, Honda Manufacturing). All IT systems, data centers, networks, and applications. Physical facilities, including manufacturing plants, warehouses, and offices.

Employees, third-party vendors, and suppliers involved in ope

16.3 Policy Statement

Honda shall maintain a robust, enterprise-wide disaster recovery strategy that includes:

Business Impact Analysis (BIA) to identify critical functions.

Risk assessments to assess threats (natural disasters, cyberattacks, pandemics, etc.).

Disaster recovery planning includes defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Redundant systems and geographically diverse backups to ensure recoverability.

Communication plans to inform stakeholders.

Regular testing of DR plans to verify effectiveness.

Continuous improvement based on test results and incident reviews.

16.4 Roles and Responsibility

Executive Leadership Approve and fund disaster recovery initiatives. Provide strategic oversight.

Global Risk Management Own and maintain the DR policy. Coordinate audits and risk reviews.

IT Disaster Recovery Team Design, implement, and maintain recovery plans. Monitor the health and performance of the DR system. Conduct regular recovery tests.

Plant Managers / Site Operations Develop localized recovery plans. Coordinate facility-specific risk mitigation.

All Employees Follow instructions during a disaster event. Complete assigned disaster response training.

16.5 Disaster Categories

Natural Disasters: Earthquakes, floods, hurricanes, and wildfires, etc.

Technological Disasters: Hardware failures, data center outages, software corruption.

Cybersecurity incidents: Ransomware, DDoS attacks, data breaches.

Man-made Disruptions: Terrorist acts, sabotage, civil unrest.

Pandemics/Epidemics: Disruptions from infectious disease outbreaks.

16.6 Recovery Plans

IT Systems Backup and replication using cloud and off-site storage. Data center failover to redundant sites. Restore network and system within RTOs.

Manufacturing Alternate production facilities for critical components. Supply chain contingency contracts. Real-time monitoring of operational status.

Communications Multichannel alerts (SMS, email, internal apps). Public relations response through designated spokespersons. Coordination with local and national authorities.

16.7 Testing and maintenance

DR plans must be tested annually or after major changes.

Types of testing include tabletop exercises, simulations, and full-scale failures.

All test results must be documented and used to update the DR strategy.

16.8 Training and Awareness

All employees must undergo annual disaster awareness training.

DR team members require specialized technical training.

New hires must be briefed on DR procedures during on boarding.

16.9 Compliance and Auditing

DR compliance will be evaluated annually by the Internal Audit Office.

All DR efforts must comply with:

ISO 22301 (Business Continuity)

ISO/IEC 27001 (Information Security)

Local laws and regulatory requirements.

Chapter 17

Artificial Intelligence Policy

17.1 Scope

This policy applies to all Honda employees and affiliates.

17.2 Safeguards

Honda is committed to full compliance with applicable laws related to the use of artificial intelligence in the countries in which Honda provides products and services. Additionally, Honda is committed to the ethical use of artificial intelligence. This Artificial Intelligence Use Policy ("AI Policy") outlines Honda's requirements with respect to the adoption of all forms of artificial intelligence at Honda. Such artificial intelligence adoption includes use for business efficiencies, operations, and inclusion in Honda's products and services.

This Policy is applicable to all Honda directors, officers, board members, employees, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of Honda. The Ethics Board at Honda is responsible for the enforcement of this Policy.

17.3 Guiding Principles

The intent of this Policy is to provide general guidance on the use of AI at Honda so that Honda can leverage the use of AI as a tool while ensuring it continues to meet legal obligations and act in an ethical manner. The use of AI at Honda should never compromise Honda's core values or introduce undue risk to the organization. Rather, the use of AI at Honda should be focused on improving business efficiencies and enhancing Honda's ability to fulfill its mission.

It is important to remember that Honda is a global organization. Honda has entities and staff globally and provides its products and services to customers globally as well. Accordingly, this Policy provides overarching guidance based on global standards for the use of AI. Honda Representatives should be cognizant when using AI at Honda that they think about the global impact of their decision to use AI, as a similar use of AI in some countries may not be permitted in others.

This Policy is not intended to address every use of AI at Honda by a Honda Representative. There are certain business departments and functions at Honda that bear more considerations and potential risks. Before using any AI at Honda—whether for personal business tasks such as writing an email or more complex business processes such as analyzing datasets - you should consult with your manager and seek guidance. Also, please see Prohibited Uses in Section III below for situations in which AI may not be used at Honda, and High-Risk Use of AI Systems in Section V below for situations in which extreme caution is required when considering using AI.

In addition, there are certain Embedded AI Tools used in existing approved Honda software that do not require additional approval for use. For example, the use of Microsoft Word in which Microsoft Word has embedded an AI tool to check spelling or grammar. The use of Embedded AI Tools in approved software at Honda is permitted, provided those software tools are aligned with previous general business uses. New AI tools may be approved upon request to the AI committee.

A list of existing software tools with Embedded AI Tools that are approved at Honda:

1. Microsoft 365.
2. Microsoft CoPilot inside of Honda systems.
3. TensorFlow and TensorFlow Lite.
4. Qualcomm Neural Network (QNN) software development kit (SDK).
5. NVIDIA DeepStream.
6. MicroAI AtomML.

When third-party software, services, or contractors are utilized or employed, any AI usage by software used by these parties or services must be noted and evaluated carefully. Contracted services that utilize AI technology should be considered in the same light as individual AI usage. Consult with the Legal Department about the inclusion of an AI-specific clause in any vendor or contractor agreements.

The following principles must be followed when considering using an AI system at Honda:

1. The use of an AI system should primarily focus on completing departmental goals as directed by company leadership. Except for the use of an Embedded AI Tool in a software system approved for use at Honda, any use of a new AI System at Honda must be approved by the AI Committee.
2. Individuals using an AI system must have expertise in the subject matter for which the AI is used. AI is to be utilized as a tool and is not a substitute for expertise. For example, if using AI for coding, the individual deploying the AI must have expertise in coding.
3. All AI-generated content (writing, datasets, graphs, pictures, etc.) must be thoroughly reviewed by an individual with expertise to evaluate such content for accuracy as well as general proofing and editing. AI-generated content should be viewed as a starting point, not the finished product. Like any content at Honda, AI-generated content should conform to the look and feel of the Honda brand and voice.
4. Any use of an AI system must have clear objectives for the AI use as a tool and business-accepted data sets from which the AI draws. If the data sets that the AI is using are not accurate, then the information AI provides will not be accurate.
5. AI systems are trained on data that may contain inherent bias. Users of these systems are responsible for reviewing any AI-produced content for bias and correcting it as necessary.
6. Non-public Honda information must never be put into an open AI system.
7. Honda Representatives must document all AI systems they are utilizing and for what functions. Tracking the use of AI is not optional and is part of your job. Documentation of specific AI Embedded Tools in an approved existing software tool when using that tool as intended is not required. Discuss the process for tracking the use of AI systems with your department head.
8. The use of an AI system must be documented to capture institutional knowledge. For example, if AI is used to create code and included in a larger section of code, there must be documentation as to which code section is AI-derived and who reviewed it.
9. The use of an AI system must meet any terms of use or contractual limitations. Contractual restrictions or terms of use may restrict Honda's use of an AI system that would otherwise be legally compliant and ethically sound. For example, an AI system's terms of use may require the use of certain disclaimers in certain use situations or prohibit the use of the AI system to do certain tasks. Honda Representatives should have all terms or use or contracts for AI systems reviewed by the Legal Department to ensure compliance with contractual obligations in using an AI system.

10. of an AI system does not eliminate the need for other internal approvals required at Honda for the use of technology, such as a security review, privacy review, cost review and spend approval, legal review, human resources review, etc. An AI system should go through the same review and approval process as other software or services at Honda. You should also ensure within your business unit that your business leader is aware of the use of the AI system and has approved any use of the AI system, particularly for AI-generated content that will be relayed externally.

17.4 Prohibited Uses.

There are certain uses of AI that are prohibited. Unless otherwise approved by the AI committee and respective department heads, Honda Representatives are prohibited from using AI systems for any of the following activities at any time:

1. Conducting political lobbying activities is prohibited. Lobbying is defined as any action aimed at influencing a Government, Government Official, or Government Entity for any reason.

2. Using AI systems to identify or categorize customers, candidates, employees, contractors, or other affiliated entities based on protected class status is prohibited.

3. Entering trade secrets, confidential information, or personal data about any individual into an open AI system.

4. Entering any sensitive information about an individual into any AI system. "Sensitive information" includes medical, financial, political affiliation, racial or ethnic origin, religious beliefs, gender, sexual orientation, disability status, or any other protected information relating to an individual.

5. Using an AI system to obtain legal advice, including, but not limited to, creating policies for internal use or to provide to third parties.

6. Creating intellectual property that Honda desires to register and/or holds significant value to the organization.

17.5 Ethical Guidelines.

Honda desires to act in an ethical manner when using AI. Accordingly, there may be uses of AI that are legally permissible but which do not meet ethical requirements. Any use of an AI system at Honda should conform to the following ethical guidelines:

1. **Informed Consent:** Prior to inputting personal information into a closed AI system, ensure that you have obtained informed consent from the individual(s) whose personal information will be inputted.

2. **Integrity in Use:** All users of AI systems should be honest about how AI helped in getting the work done. Even if using an AI system approved by the AI Committee for an approved use, you should ensure your manager or the department requesting a task for which you are using an AI system is aware of your use of the AI system. Do not pass off AI-generated work as done by you solely. Additionally, you should ask permission if you desire to use an AI system tool to complete a task. For example, you should ask your manager and HR representative if you may use an AI system to assist in writing a performance evaluation.

3. **Appropriate Content:** Do not use company time or resources to generate content using an AI system that would be considered illegal, inappropriate, harmful to Honda's brand or reputation, or disrespectful to others.

4. **Unauthorized Use:** Do not use company time or resources to generate content using an AI system for personal use without prior approval of the appropriate department leader.

17.6 High-Risk Use of AI Systems.

There are certain uses of AI systems that are more high risk than others. As a global company, Honda is committed to complying with all AI legal requirements and guidance in the countries in which it operates. The European Union ("EU") has classified the following potential uses of AI as posing a high risk to the health and safety or fundamental rights of natural persons. Therefore, there are several additional requirements for the use of AI systems in such cases. These requirements are listed in Appendix II, with certain functions highlighted below:

1. **Personal Data in AI Systems:** AI should be used with extreme caution when inputting any personal data of an individual into a closed AI system (it is prohibited to put any personal data into an open AI system).

2. **Screening Job Candidates:** AI should be used with caution when screening any job applicants to ensure it does not adversely impact protected class members or introduce any bias. Equity and inclusion issues surrounding AI use in job screening are a potential source of litigation.

3. **Personnel Decisions:** AI should be used with caution for any use related to making decisions on promotions, retention, or similar personnel such decisions. Extreme caution should be utilized to ensure that biases (including biases found in existing data sets) are avoided.

4. **Enrollment Decisions:** Extreme caution should be utilized if using AI in any manner related to evaluating potential candidates for admission into an academy, internship or apprenticeship program, or any other Honda program.

17.7 General AI System Use Standards and Use Approval.

Except for AI Embedded Tools in approved software, all uses of AI systems must be approved by the AI Committee prior to use to ensure such AI system use meets the following principles:

1. **Lawful:** The use of AI systems must comply with all applicable laws and regulations, as well as any contractual obligations, limitations, or restrictions.

2. **Ethical:** The use of AI systems must adhere to ethical principles, be fair, and avoid bias.

3. **Transparency:** There must be clear objectives for the use of an AI system and documented oversight of such use, which is recorded and captured for institutional knowledge. Disclosures of the use of AI in any AI-assisted content generation must be made when required by law or contract, or when required by Honda.

4. **Necessity:** The use of AI systems must be for a valid business purpose to improve Honda's business efficiencies and support the organization's mission. The use of AI is not a substitute for human critical thinking or expertise and should not require Honda to incur an unnecessary expense without any true benefit.

Prior to submitting a request to the AI Committee for the use of an AI system, a requester should first obtain the approval of their manager. In addition, in evaluating whether to make a request, the requester should ensure that the AI system use, if approved, would conform with the guidelines in this Policy, prior to submitting said request. Requests for the use of an AI system should follow the SOP here [HYPOTHETICAL-LINK-TO-SOP].

17.8 Training.

All Honda Representatives who interact with AI systems must be trained on this Policy. Additionally, specific departments or functions at Honda may require more specific training on the use of AI systems for their department or function when more high-risk.

17.9 Reporting Non-Compliance.

Honda directors, managers, employees, and agents aware of any conduct that may violate this Policy have a responsibility to report it. Individuals are encouraged to make reports through normal reporting relationships beginning with their manager. All reports of suspected misconduct or non-compliance will be investigated by the AI Committee, Legal Counsel, Human Resources, or other appropriate parties. Unless acting in bad faith, Honda employees will not be subject to reprisals for reporting potential violations.

If Honda determines that a Honda Representative has failed to comply with this Policy after an investigation concludes, then the Honda Representative will be subject to disciplinary action, up to and including termination.

Appendix A

Glossary

A.1 Terms & Acronyms

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. .

Audit A check to make sure rules are being followed, often done by reviewing documents, systems, or interviews..

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. .

Backdoor A hidden way into a system or program that can be used to bypass normal security..

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. .

Browser Extension / Plug-in Software add-ons that extend the functionality of a web browser; unauthorized use can create security vulnerabilities..

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. .

Closed AI System An AI system where the input provided by one user is used to train the AI model. Input data from the user is isolated from other users, and the data is considered more secure..

Compliance Following all the rules and policies set by the company..

Confidential Data Private or secret information that should not be shared without permission..

Confidential Information Data that must be kept private, such as employee records, customer data, or financial reports..

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

Content Filtering A technology that restricts access to certain websites or online material based on predefined policies..

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 Breach When private information is stolen, leaked, or shared without permission..

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. .

Dependencies Extra parts or tools a piece of software needs to work, which may also carry risks..

Digital Infrastructure The computer systems, software, and networks that a company uses to run its business..

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. .

Embedded AI Tools AI tools embedded in existing software tools approved and used at Honda and which do not require approval for use from the AI Committee..

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.

Government Entity Any entity controlled by a government in whole or part. This includes Government-owned or controlled (whether whole or partial ownership or control) commercial enterprises, institutions, agencies, departments, instrumentalities, and other public entities, including research institutions and universities..

Government Official Any officer or employee of a Government Entity, an official of a political party, a candidate for political office, officers and employees of non-governmental international organizations, and any person with responsibility to allocate or influence expenditures of Government funds. This includes data scientists and researchers who are employed by a government or a Government Entity. Employees at government organizations are considered Government Officials regardless of title or position..

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

Honda Representatives All Honda directors, officers, board members, employees, contractors, representatives, resellers and sub-resellers, distributors and sub-distributors, affiliates, agents, and any person or entity performing services for or on behalf of Honda..

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. .

IT Helpdesk The department responsible for providing technical support, including reporting of suspicious emails and system issues..

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

Legal Action When a company uses the law to get payment or justice if another party breaks a contract..

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. .

Monitoring The process by which the IT department observes and reviews user activity on company systems to ensure policy compliance..

Non-public Honda Data Any information that, if disclosed, could violate the privacy of individuals, government regulations or statutes, could jeopardize the financial state of Honda, could injure its reputation, or could reduce its competitive advantage..

Open AI System Open AI System: An AI system where the input provided by all users is used to train the AI model. Input data from all users is not private and may be revealed to other users..

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

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

Patch/Update Schedule A regular plan for fixing or updating software to make sure it stays safe..

Personal Information Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household..

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. .

Proprietary Information Company-owned information such as trade secrets, manufacturing processes, and internal reports that must not be shared externally..

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. .

Reputation Management Steps a company takes to protect or fix its image after a public problem..

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. .

Security Review A close check of software or systems to find and fix possible security problems..

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. .

Social Media Online platforms like Facebook, Twitter, LinkedIn, and others that allow users to share information or content. At HMIN, their use must align with approved business communication standards..

Third Party A company or group that is not part of Honda but works with Honda, such as vendors, contractors, or service providers..

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. .

Unauthorized Software Any program or application not approved for use by the company's IT department..

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. .

Appendix B

Artificial Intelligence

This appendix outlines the approved artificial intelligence (AI) techniques and approaches authorized for use in Honda systems and infrastructure. It also identifies the tools through which these techniques are deployed, describes the primary use cases, and specifies associated constraints and security considerations. This appendix will not be comprehensive, but rather a guideline for appropriate conduct. Ask your supervisor if you have questions about AI techniques and approaches.

B.1 Supervised Learning.

Supervised learning models are authorized for deployment in perception, classification, and predictive diagnostics applications.

1. **Examples:** Convolutional Neural Networks (CNNs), Support Vector Machines (SVMs), Decision Trees, Long Short Term Memories (LSTMs).
2. **Tools Used:** TensorFlow/TensorFlowLite, Qualcomm Neural Network SDK, and NVIDIA DeepStream.
3. **Use Cases:** Driver assistance perception (vehicle, pedestrian, traffic light detection), predictive maintenance for rotating equipment, and in-cabin gesture recognition and personalization.

B.2 Unsupervised Learning.

Unsupervised learning models are to be used primarily for anomaly detection and pattern recognition in cases where labeled data is scarce.

1. **Examples:** Autoencoders, Clustering (K-Means, DBSCAN), Principal Component Analysis (PCA).
2. **Tools Used:** MicroAI AtomML and TensorFlow Lite.
3. **Use Cases:** Learning normal operational patterns of ECUs, motors, and sensors, and detecting abnormal behavior in factory robots or HVAC systems.

B.3 Reinforcement Learning.

Reinforcement learning models are permitted for simulation and training purposes only; not allowed in direct control loops in production unless human oversight is guaranteed.

1. **Examples:** Q-Learning, Deep Q-Networks (DQN), Proximal Policy Optimization (PPO).
2. **Tools Used:** TensorFlow.
3. **Use Cases:** Simulated driver behavior models and manufacturing flow optimization.
4. **Restrictions:** Reinforcement learning models may not autonomously update policies in production. Additionally, model deployment requires an audit of reward signal safety and risk tolerance.

B.4 Deep Learning.

Deep learning techniques are authorized when used with approved frameworks and hardware platforms that support explainability or low-level model inspection.

1. **Examples:** CNNs, recurrent neural networks (RNNs), Transformers, Attention Mechanisms.
2. **Tools Used:** TensorFlow/TensorFlow Lite and ONNX Runtime via QNN SDK or DeepStream.
3. **Use Cases:** In-vehicle visual perception and speech interfaces and lane following and environmental awareness in advanced driver assistance systems (ADAS).

B.5 Logic and Knowledge-Based Approaches.

Knowledge-based and symbolic reasoning systems are approved in scenarios requiring rule-based decisions, traceability, and legal compliance.

1. **Examples:** Knowledge graphs, deductive engines, inference rules, and expert systems.
2. **Tools Used:** Microsoft Copilot (when deployed with restricted access to internal documentation systems) and embedded rule engines within AtomML environments.
3. **Use Cases:** Repair recommendation systems and internal support automation using CoPilot in code review or documentation workflows.

B.6 Statistical and Probabilistic Methods.

Statistical inference and probabilistic modeling techniques are permitted for decision support and analytical modeling. These approaches form the foundation of many AI model components.

1. **Examples:** Bayesian Networks, Gaussian Mixture Models, Kalman Filters, Markov Chains.
2. **Tools Used:** TensorFlow (Bayesian layers) for probabilistic neural networks and MicroAI AtomML for running lightweight, statistical model-based anomaly detection on-device.
3. **Use Cases:** Sensor fusion in ADAS and forecasting fuel efficiency or component wear.

B.7 Tool-Specific Constraints and Conditions.

1. **Microsoft CoPilot:** Approved only in isolated developer environments. Output must not be used in production decision systems without validation.
2. **TensorFlow/TensorFlow Lite:** Permitted for training and edge inference. Inference models must be quantized, validated, and signed before deployment.
3. **Qualcomm Neural Network SDK:** Permitted only for inference on validated Snapdragon-based hardware. Backend layer assignments must be logged.
4. **NVIDIA DeepStream:** Approved for video-based inference systems. Pipelines must be locked from runtime modification and only use validated ONNX or TensorRT models.
5. **MicroAI AtomML:** Permitted for both training and inference at the edge. Runtime adaptation must be sandboxed, with thresholds and feedback loops tuned to prevent drift or overfitting.