DIAMOND HANDS HOLDING INC.

TO: Jake Bulim, Evan Battaglia, John Smith, Steve Smith, Katie Tylerr

FROM: Ethan Byrd, Cybersecurity Compliance Consultants

SUBJECT: Security Services Directory Recommendation and Plan

DATE: November 3, 2025

Dear Executives and Stakeholders,

My name is Ethan Byrd, the Cybersecurity compliance consultant at Diamond Hands Holding Inc. (DHHI) and since our last meeting to discuss information security strategies, I was tasked with locating a cybersecurity framework plan that met the needs of the company. The information provided in this plan stems from the NIST Cybersecurity Framework (CSF) 2.0 document that was written and published by the National Institute of Standards and Technology (NIST). Other frameworks such as ISO/IEC 27001 and CMMC 2.0 were considered as well but I found that the CSF 2.0 best fits the company's needs.

Attached to this document you will find a security services development plan that was crafted using the CSF 2.0 documentation. CSF provides a robust framework to organizations looking to manage their cybersecurity risks. No matter the size or sector, CSF seeks to help companies better understand their assets and the different actions that must be taken based on different risk stances and system priorities. It does so by providing core functions and components that the company must follow concurrently to detect and prevent incidents. It also goes beyond just providing the framework by providing online resources and other means of improvement.

Based off the above information that I compiled, I found this cybersecurity framework to be the best fit for DHHI to build out the directory. There is a reason that NIST publications are used as the standard for all technology and cybersecurity practices. They provide the structure and guidelines that are built upon field tested research, consistency and resilience, all of which are attributes that will greatly enhance DHHI's cybersecurity framework.

Sincerely,

Ethan Byrd

Cybersecurity Compliance Consultant

Ebyrd13@students.kennesaw.edu

678-630-9716 (Ext. 216)

Security Services Directory Development Plan

1.0 Purpose

The purpose of this document is to provide an essential plan for DHHI to build a security plan based on the organization's current security, missions, and directive. DHHI will have the flexibility to implement and build upon this plan based on their future needs. This plan will follow all operational, legal, and sector requirements. These requirements and current assets will be documented to ensure smooth implementation of new and updated assets and to track the system development lifecycle (SDLC). All of this will be backed up using DHHI's core mission and aligning it with the NIST Cybersecurity framework to ensure a holistic and secure approach.

2.0 Evaluation

All systems and policies will require a quarterly evaluation by the Chief Information Officer's (CISO) Departmental Directors and other Information Security team members.

Last review date: November 3rd, 2025
Next Review Date: January *TBD*, 2026
Version: Marquise 1.0
Changes made by: Ethan Byrd

3.0 Roles and Responsible Personnel

Executive Board
Jake Bulim: CEO

- Leads the organization by setting a high standard and guiding the company to follow its mission.

Evan Battaglia: CISO

- Leads the company's information security strategies and will work alongside other officers and Information security team members on a quarterly basis to review all assets and their SDLC and decide if changes need to be made to the company.

John Smith: CFO

- Leads the company financial team, along with budgeting the year out to ensure room for growth and unknown allocations.

Steve Smith: CTO

- Leads the company's technology strategies and will work along with the CISO and Information security team members on a quarterly basis to review all assets and their SDLC and decide if changes need to be made to the company.

Katie Tyler: COO

- Leads the day-to-day operations and helps find and promote the need for efficiency and productivity within the company.

VIPS
Stacy Smith: Assistant Technology Officer
Melissa Stark: Assistant Operations Officer
Johnny Appleseed: Assistant Finance Officer

Executive Security Team
Michael Peterson: Cyber Threat Intelligence Director (CTI)

- Lead for data analysis and gathering to produce cyber insight to help support the company's risk stance and incident response.

Chase Johnson: Cyber Triage and Forensics Director (CTF)

- Leads cyber forensic team to investigate and report from potential or past threats to the company.

Dave Frey: Digital Forensics Incident Response Director (DFIR)

- Leads the search for computer forensic searches within endpoints to identify the root cause of threats and the reason for compromise to protect the company.

William Jones: Incident Response and Contingency Coordination Director (CIR)

- Works to fix and restore company functions after a declared incident.

Issac Wilson: Lead Security Operations Center Director (SOC)

- Manages compliance for DHHI's security operations center.

Steve Smith: Identity Access Provision Director (IAM)

- Oversee all organizational user access controls and request to implement the principle of least privilege.

** All user information such as email and phone numbers will be stored in a company directory database to prevent any unnecessary privacy risks for high-ranking users.*

4.0 System Operational Status

DHHI's operational and information security status is: **Undergoing a major modification**

The status is set to **Undergoing a major modification** due to the overhaul of security services plan along with the transition to a new building to ensure asset protection.

5.0 Plan

The plan is to compile all the assets that DHHI owns such as: Physical property (Warehouse, Office Building), Intellectual Property (In-house systems and ideas), hardware, software, and data and assess each of those against different considerations. The considerations we will be using are methods to obtain data, tools/software needed to access the data, risk tolerance, risk appetite, and financial value/risk. Each of these considerations will be considered on a quarterly basis with the CSI, CTO, and Information Security team. With these meetings, when an asset is deemed to still be valuable to the company and will remain in the directory, the organization must then decide if the policies put in place have appropriate Governance, risk and compliance measures (GRC). If an asset is to be phased out, the team will then need to discuss if something needs to take its place or do we have no more need for the theoretical service. This directory will slowly be updated with the addition or removal of an asset and must be accordingly updated with the version and who changed the documentation.

These meetings will have an outlined approach to verify the assets we have and if they will remain a part of DHHI.

- **Pre-Meeting:** Each member of the meeting will gather the assets they use on a day-to-day basis along with gathering information on the assets such as cost, developer support, competitors, and other meaningful information.
- **Initial Discussion:** Each member of the meeting will provide the current hardware, software, and other tools they use on a day-to-day basis to have a living list of our assets. Each member of the meeting will go over the assets they provided and discuss if they find the asset is still relevant or not, or if they think new assets should be implemented into DHHI.
- **Consideration**: After reviewing current and potential assets, the assets will be considered by using metrics such as methods to obtain data, tools/software needed to access the data, risk tolerance, risk appetite, and financial value/risk. It must also align with DHHI's mission and have a strong connection with the NIST Cybersecurity framework.
- **Final Choice**: After the executives and team have thoroughly reviewed each asset in depth, the final choices for each asset will be made and the newest version of the document will be published.

6.0 Plan Validation

Once the newest version of the SSD has been published, the SSD will be validated and applied by means of budget re/allocation, policy application or rework, and ensuring the plan aligns with core mission and values of the company.

- **Training:** The information security team must ensure there is proper training for all newly added assets and must also review that all prior training is still up to standard or needs to be updated based off new policies or if the application has been updated. This can come in the form of one-on-one training for more in-depth usage or seminars for a general audience approach for a more base-level usage and understanding. The team must

also track whether the training is effective, whether that be by feedback forms, word of mouth, or if users have questions regarding the asset even after training.

- **Policies:** The information security team must ensure that proper acceptable use policies (AUP) are put into place for all new assets along with reviewing older policies that need to be modernized or replaced. The team must also track whether the policy is effective, by measuring the number of security incidents, or quizzes to confirm policy knowledge
- **Testing Periods:** Before new assets can be rolled out, the information security must test them in a controlled environment to mirror business operations to ensure proper time to observe different performance metrics, along with ensuring the asset meets all GRC requirements, using the NIST cybersecurity framework to validate this.
- **Quarterly Review:** After assets have been implemented along with new and updated training, and policies, the CISO, CTO, and information security team must meet on a quarterly basis (date subject to approval). In these meetings the team will not only discuss current assets and the need to be updated but will also discuss whether the training and policies put into place were effective by taking the key performance indicators (KPIs) collected (quizzes, feedback) and deciding if the collected data shows improvement or the need for stronger training and policies.

These review and validation phase will serve as a great way for DHHI to stay on top of its SDLC and ensure that all assets are following the mission of the company and the framework set by NIST.

7.0 Summary of Approach

1. The entire document is built upon the foundation laid out in the NIST Cybersecurity Framework (CSF) 2.0. I chose this document due to NIST playing a familiar role within this organization now, allowing for easy implementation alongside other used publications. It will help DHHI in managing its risk, governance, and ensure directives from the top down.

2. I defined a clear list of people who will be involved in this transitional period, along with the role they will play, creating a clear hierarchy. The executives will provide strategic insight, as well as making the final decisions, while the executive security team will manage these operational assets. Clear and defined roles between leadership and the information security team will help with collaboration and ensure all changes align with the company's mission.

3. The SSD outlines a well-defined approach to meetings when discussing assets. Giving each meeting attendee a well-defined job of what to do before, during, and after the meeting. These meetings will cover each asset in depth, leading to conversations on whether the asset is still needed, or if an asset is needed to cover a new vulnerability.

4. Ensuring validation after the meeting must remain an active part of this transitional period. After planning and testing, assets, policies, and training will be rolled out to ensure compliance with all new assets. These will be reviewed on a quarterly basis to ensure compliance is still met with policies, training, and asset protection. Basing how DHHI is doing based on KPIs will ensure the company maintains compliance with DHHIs mission and legal standards.

8.0 Security Services Directory Table

Service/Tools	Description	Owner	Frequency	Justification	Cost
Cameras	Surveillance and security system used to monitor offices and factories.	IT/ Information Security Team	Quarterly	Supports facility access control, deters theft, and aids in forensic investigations.	$2,000–$5,000 /yr
Laptops	Employee devices configured with remote system, monitoring, and encryption	IT/ Information Security Team / All Employees	Quarterly	Ensures secure access to corporate resources and data mobility with encryption and MDM.	$1,000 per device avg
Policy and Training Creation/Audit	Group policies and training used to provide employees with knowledge and awareness of safe technology usage	IT/ Information Security Team / HR	Quarterly	Ensures compliance with security frameworks (NIST, ISO 27001) and reduces user error risk.	$500–$1,000 /session
Phishing Simulation	Phishing campaign used to assess employee awareness and to improve future outcomes	IT/ Information Security Team	Quarterly	Reduces risk of credential theft and social engineering by testing user response.	$2,000–$4,000 /yr
Automated Penetration Testing	Either a continuous or set testing times to exploit vulnerabilities in the system	IT/ Information Security Team	Quarterly	Identifies exploitable vulnerabilities and validates patch management effectiveness.	$10,000–$20,000 /yr
Preventative Endpoint Security	Zero trust protection, disallowing permission escalation	IT/ Information Security Team	Quarterly	Blocks unapproved applications and ransomware using default-deny model and ringfencing.	$5–$10 /device /mo
Data Loss Prevention	Used to monitor data exfiltration	IT/ Information Security Team	Quarterly	Prevents sensitive data from leaving the organization and enforces compliance rules.	$8–$12 /user /mo
Network Security Assessment/ Management	Constant audit of network tools such as firewall and running vulnerability scans	IT/ Information Security Team	Quarterly	Detects and remediates misconfigurations and exposed services before exploitation.	$4,000–$8,000 /yr

Third party/Legal Assessment	Review risk assessment or used to review internal or vendor incidents	Legal	Quarterly	Reduces third-party risk and ensures data-handling agreements meet legal obligations.	$2,000–$6,000 /yr
Cloud Storage and Security	Backup the cloud and allows for MFA protection along with encryption	IT/ Information Security Team	Quarterly	Protects data integrity and availability while meeting compliance and disaster recovery goals.	$3–$6 /user /mo
Forensic Tools	Software and hardware used to investigate cyber incidents and collect digital evidence	IT/ Information Security Team	Quarterly	Enables root-cause analysis and evidence preservation for post-incident response.	$1,000–$5,000 /yr
Vulnerability Management Platform	Centralized system for tracking, and prioritizing vulnerabilities	IT/ Information Security Team	Quarterly	Improves visibility of system weaknesses and ensures timely remediation of critical vulnerabilities.	$6,000–$12,000 /yr
SIEM / Log Monitoring	Security Information and Event Management tool for real-time log analysis	IT/ Information Security Team	Quarterly	Detects anomalies and correlates events for early detection of cyber incidents.	$8,000–$15,000 /yr
Patch Management System	Automated platform for deploying OS and software updates organization wide.	IT/ Information Security Team	Quarterly	Reduces exposure to known vulnerabilities by ensuring consistent patch deployment.	$3–$7 /device /mo
Incident Response Plan Testing	Tabletop and live simulations to validate IR plans and improve response readiness.	IT/ Information Security Team	Quarterly	Ensures organization can respond effectively to breaches and minimize downtime.	$2,000–$5,000 /test
Email Protection	On-premises or vendor system used to filter and/or block spam emails	IT/ Information Security Team	Quarterly	Enhances email protection and prevents malicious payload delivery to users.	$4–$8 /user /mo

AI/LLM Usage Statement

Answer Yes/No	In preparing for this assignment, I used assistance for the checked items	Prompt Used/Comments
No	Planning/Outlining: I used external LLM/AI assistance to plan or outline the topic.	NA
No	Research: I used external LLM/AI assistance to perform preliminary research.	NA
Yes	Composition of Text: I used external LLM/AI assistance to compose any submitted text.	I used external LLM to generate cost for the SSD table.
No	Creation of Graphics or Videos: I used external LLM/AI assistance to create graphics or videos included in the submission.	NA
No	Conceptual or Critical Review: I used external LLM/AI assistance to perform a conceptual or critical review of the draft work.	NA
No	Spell Checking and Grammar Review: I used external LLM/AI assistance to perform spell checking or grammar review.	NA
No	Assistance from Other People: I received assistance from another person.	NA
No	Reuse of Previous Work: I reused by copying or repurposing work submitted for this or another course. If any use is included, how was it used, and did you seek permission from the instructor in advance?	NA
Yes	Certification: I affirm that all statements above are accurate and that the submitted work complies with the course's academic integrity policies.	