Security Audit Checklist

18 May 2023 / Eula Bassett

Complete

Score	**96.08%**	Flagged items	**2**	Actions	**3**

Audit Title	Annual Security Audit Report
Client/Company Name	Lard Corporate Holdings, Inc.
Location	Massachusetts, USA (42.4072107, -71.3824374)
Conducted on	18.05.2023 13:00 PST
Conducted by	Eula Bassett

Flagged items & Actions

2 flagged, 3 actions

Flagged items

2 flagged, 2 actions

Security Audit / Compliance

Are vendor and third-party risk management plans in place? No

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:28 PST | Created by SafetyCulture Staff

Create vendor and third-party risk management plans and have them approved before the end of Q4 2023.

Security Audit / Visitors Vehicle Access

Are visitors announced? No

While we always remind our employees to inform us beforehand of any visitors coming in, there are still some cases where this isn't applied.

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:32 PST | Created by SafetyCulture Staff

Enforce stricter measures on visitor management and logs.

Other actions

1 action

Security Audit / Employee Awareness and Training

Are employees provided with security awareness training? Yes

However, our training materials and courses need to be updated before this quarter ends to account for the recent changes in our security policy.

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:26 PST | Created by SafetyCulture Staff

Update security awareness training.

Security Audit	2 flagged, 3 actions, 96.08%

Progress through the following sections, answering each question. When an item is non-compliant or marked as fail, be sure to add notes and/or media as evidence.

Access Controls

100%

Are user accounts created with strong passwords?	Yes
Is multi-factor authentication (MFA) implemented for privileged accounts?	Yes
Are access rights regularly reviewed and revoked for terminated employees?	Yes
Does the facility use an automated access control system?	Yes
Are card readers utilized at all access points?	Yes
Are card readers securely fastened and in good working order?	Yes

Photo 1

Network Security

100%

Is a firewall in place to control incoming and outgoing network traffic?	Yes
Are intrusion detection and prevention systems (IDPS) deployed?	Yes
Are network devices regularly patched and updated?	Yes

Data Protection

100%

Is sensitive data encrypted both at rest and in transit?	Yes
Are regular data backups performed and tested for recoverability?	Yes
Are data access and usage monitored and logged?	Yes

Physical Security

100%

Are all the doors and windows secure and able to be locked?	Yes
Are physical access controls implemented, such as access badges or biometric systems?	Yes
Are server rooms and data centers secured with appropriate physical safeguards?	Yes

Photo 2

Is after-hours access to server rooms monitored/controlled?	Yes
Are the external walls fit for purpose and are they secure?	Yes
Is there a visitor log and escort policy for visitors entering restricted areas?	Yes
Are perimeter doors alarmed?	Yes
Are alarms active during the day or are areas shut off?	Yes
Is there a regular lock-up routine?	Yes
Are perimeter doors supported by cameras?	Yes
Are computers marked with serial numbers or company information?	Yes
Is an intrusion alarm system used in the facility?	Yes
Is the intrusion alarm system in good working order?	Yes
Does the alarm system have a power backup?	Yes
Are fire prevention and suppression systems in place?	Yes
Are power backups available?	Yes
Is environmental monitoring implemented?	Yes

Incident Response

100%

Is an incident response plan in place and regularly tested?	Yes
Are security incidents and breaches promptly reported and investigated?	Yes

Is there a process for notifying affected parties in the event of a data breach?	Yes

Employee Awareness and Training

1 action, 100%

Are employees provided with security awareness training?	Yes

However, our training materials and courses need to be updated before this quarter ends to account for the recent changes in our security policy.

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:26 PST | Created by SafetyCulture Staff

Update security awareness training.

Do they understand the importance of vigilance and challenging suspicious activity?	Yes
Do employees sign an acceptable use policy regarding information security?	Yes
Are employees regularly reminded of security best practices and policies?	Yes
Are employees aware of and compliant on how to report suspicious activities or incidents?	Yes

For reference, see attached file for the SOPs on Security Incident Reporting.

SOPs on Security Incident Reporting.pdf

Compliance

1 flagged, 1 action, 80%

Is the organization compliant with relevant security regulations and standards?	Yes
Are security audits conducted by third-party assessors periodically?	Yes
Is there a process for addressing security audit findings and implementing corrective actions?	Yes
Are all security policies and procedures documented?	Yes
Are vendor and third-party risk management plans in place?	No

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:28 PST | Created by SafetyCulture Staff

Create vendor and third-party risk management plans and have them approved before the end of Q4 2023.

Electronic Security

100%

Is there ample/well-maintained lighting?	Yes
Are cameras installed?	Yes
How many cameras are functional?	25
How many cameras are inoperable?	None
Are cameras managed by security, IT, facilities, or others?	Security department
Are monitors clear?	Yes

Attach photos and other relevant files as evidence.

Photo 3

Photo 4

Information Security

100%

Is there an effective information security strategy?	Yes
Is there an effective IT strategy?	Yes

Visitors Vehicle Access

1 flagged, 1 action, 80%

Is there an access control system in place for visitor vehicles?	Yes
Do visitors have to show ID?	Yes
Are visitors announced?	No

While we always remind our employees to inform us beforehand of any visitors coming in, there are still some cases where this isn't applied.

To Do | Assignee SafetyCulture Staff | Priority Low | Due 26.05.2023 00:32 PST | Created by SafetyCulture Staff

Enforce stricter measures on visitor management and logs.

Are visitors required to park in certain areas?	Yes
Are there passes issued? If yes, describe the types of passes issued.	Yes

We currently have four types of passes: Temporary Visitor Pass (e.g. single-day visit), Contractor Pass (for contractors or external service providers), VIP Pass (for high-profile visitors or individuals with special status), Long-term Visitor Pass (for visitors who will be regularly accessing the facility over an extended period)

General Facility Impressions and Security Posture

What is the estimated volume of daily visitors?	The estimated volume of daily visitors to the facility is approximately 50-100 individuals

Have there been security problems in the past? Describe in detail.

In the past, the facility has experienced several security problems. These include unauthorized access attempts by individuals posing as visitors, theft of company equipment from unsecured areas, and a data breach resulting from a compromised user account. These incidents highlight the need for improved visitor management, stricter access controls, and enhanced user account security measures.

What are the biggest threats to security?

The biggest threats to security at the facility are unauthorized access by individuals with malicious intent, physical theft of assets, data breaches or unauthorized disclosure of sensitive information, and potential disruption of critical systems through cyber-attacks. Additionally, insider threats and social engineering attacks are also significant concerns that need to be addressed.

What assets at the facility need to be protected?

The facility houses several assets that require protection, including sensitive company data, intellectual property, physical infrastructure, server rooms containing critical systems, computer equipment, and other valuable resources. It is essential to safeguard these assets to prevent unauthorized access, theft, or damage.

Completion

Summary of Findings

Overall, the security audit revealed that the facility has implemented various security measures effectively. Strong passwords and multi-factor authentication are in place for user accounts, and regular access rights reviews are conducted. The facility utilizes an automated access control system with card readers at all access points. Network security measures, such as firewalls and intrusion detection and prevention systems, are deployed and regularly updated. Sensitive data is encrypted, and data backups are performed and tested regularly. Physical security controls, including secure doors and windows, access controls, and alarm systems, are implemented. Incident response procedures and compliance with security regulations and standards are established. Security awareness training is provided (but yet to be updated) to employees, and security policies and procedures are documented.

Remediation and Action Plans

- Strengthen visitor management processes to prevent unauthorized access attempts.
- Implement additional security measures to mitigate the risk of theft and unauthorized disclosure of assets.
- Conduct and update periodic security awareness training and reminders for employees to reinforce best practices and reporting procedures.
- Strengthen vendor and third-party risk management plans to ensure their compliance with security requirements.

Date of Next Audit	Immediate follow-up: November 15, 2023. Next annual audit: May 20, 2024

Auditor's Name and Signature

Eula Bassett
19.05.2023 22:01 PST

Media summary

Photo 1

Photo 2

Photo 3

Photo 4

SOPs on Security Incident Reporting.pdf