Audit Checklist 2024-05-10 #1

Glow Clothing - San Lorenzo 3175 Eldorado

# Controls Verification Checklist

Select “yes” or “no” to answer the question: Does Glow Clothing currently have this control?

| **Yeah** | **No** | **Control** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | Minimum privileges | *Currently, all employees have access to customer data; privileges should be limited to reduce the risk of a breach.* |
|  |  | Disaster recovery plans | *There are no disaster recovery plans. These must be implemented to ensure business continuity.* |
|  |  | Password Policies | *Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.* |
|  |  | Separation of tasks | *It should be implemented to reduce the possibility of fraud/access to critical data, as the company's CEO currently runs daily operations and manages payroll.* |
|  |  | Firewall | *The existing firewall blocks traffic based on a set of appropriately defined security rules.* |
|  |  |  |  |
|  |  | Intrusion Detection System (IDS) | *The IT department needs an IDS to help identify potential intrusions by threat actors.* |
|  |  | Backups | *The IT department needs to have backups of critical data, in case*  *of an infringement, to ensure business continuity.* |
|  |  | Antivirus software | *The IT department installs and regularly monitors anti-virus software.* |
|  |  | Manual monitoring, maintenance and intervention for legacy systems | *The asset list notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is no regular schedule for this task and procedures/policies regarding intervention are unclear, which could put these systems at risk of a breach.* |
|  |  | Encryption | *Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.* |
|  |  | Password management system | *There is currently no password management system in place; implementing such a control would improve the productivity of the IT department and other employees in the event of password issues.* |
|  |  | Locks (offices, shop windows, warehouses) | *The physical location of the store, including the company's main offices, store front, and product warehouse, has sufficient locks.* |
|  |  | Closed circuit television (CCTV) surveillance | *CCTV is installed/operating at the physical store location.* |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *Glow Clothing's physical location has a functioning fire detection and prevention system.* |

# 

# Compliance Verification Checklist

Select “yes” or “no” to answer the question: Does Glow Clothing currently comply with these compliance best practices?

Payment Card Industry Data Security Standard (PCI DSS)

| **Yeah** | **No** | **Best practices** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | Only authorized users have access to customer credit card information. | *Currently, all employees have access to the company's internal data.* |
|  |  | Credit card information is accepted, processed, transmitted and stored internally, in a secure environment. | *Credit card information is not encrypted and currently all employees have access to internal data, including customer credit card information.* |
|  |  | Implement data encryption procedures to better protect credit card transaction data and touchpoints. | *The company currently does not use encryption to better ensure the confidentiality of customers' financial information.* |
|  |  | Adopt secure password management policies. | *Password policies are nominal and there is currently no password management system in place.* |

General Data Protection Regulation (GDPR)

| **Yeah** | **No** | **Best practices** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | EU. Customer data is kept private/secure. | *The company currently does not use encryption to better ensure the confidentiality of customers' financial information.* |
|  |  | There is a plan to notify EU customers within 72 hours if their data is compromised/there is a breach. | *There is a plan to notify EU customers within 72 hours of a data breach.* |
|  |  | Ensure data is properly classified and inventoried. | *Current assets have been inventoried/priced, but not classified.* |
|  |  | Enforce privacy policies, procedures and processes to properly document and maintain data. | *Privacy policies, procedures and processes have been developed and implemented among IT team members and other employees as required.* |

System and Organization Controls (SOC Type 1, SOC Type 2)

| **Yeah** | **No** | **Best practices** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | User access policies are established. | *There are currently no least privilege controls or separation of duties; all employees have access to data stored internally.* |
|  |  | Sensitive data (PII/SPII) is confidential/private. | *Encryption is currently not used to better ensure the confidentiality of PII/SPII.* |
|  |  | Data integrity ensures that data is consistent, complete, accurate, and has been validated. | *Data integrity is current.* |
|  |  | The data is available to persons authorized to access it. | *While data is available to all employees, authorization should be limited to only those individuals who need access to it to perform their jobs.* |

# Recommendations

This section sets forth recommendations related to controls and/or compliance needs that your IT manager could communicate to stakeholders to reduce risks to assets and improve Glow Clothing's security posture:

*Multiple controls need to be implemented to improve Glow Clothing’s security posture and better ensure the integrity of sensitive information, including:*

* Least privilege policy
* Disaster recovery plans
* Password Policies
* Separation of duties
* Implementing an IDS
* Continuous management of legacy systems
* Encryption
* Implementing a password management system

*To address compliance gaps, Glow Clothing needs to implement controls such as Least Privilege, Separation of Duties, and Encryption. The company also needs to properly classify assets to identify additional controls that may need to be implemented to improve its security posture and better protect sensitive information.*