Brandon Morgan

Sylena Beccles

Michael Varrella

Hikes R Us Audit Checklist

Does your staff wear ID badges?
Yes **No**

Note: Worn at all times while employees are on the clock.

Is a picture part of the ID badge?
Yes **No**

Note: Pictures on IDs are not up to date and are from when first hired.

Are authorized access levels and types (employee, contractor, visitor) identified on the badge?
Yes **No**

Note: Contractors and visitors all use the same badge labeled as a visitor.

Do you check the credentials of external contractors?
Yes **No**

Note: All contractors are required to provide credentials and identification for being there before access is granted.

Do you have policies addressing background checks for employees?
Yes **No**

Note: Before getting hired all employees go through a short background check that could be more thorough.

Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?
Yes **No**

Note: When looking through their accounts there were names of people that were not currently working there.

PHYSICAL SECURITY

Do you have policies and procedures that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facilities in which they are housed?
Yes **No**

Brandon Morgan

Sylena Beccles

Michael Varrella

Note: Certain personnel have more privileges with their badges than others. This allows only certain employees to go to certain places.

Is there an acceptable use policy put into place?
Yes **No**

Note: Policy is in place but not up to date.

Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?
Yes **No**

Note: This is identified in depth throughout their policies and procedures.

Is there a room designated as the server room where all IT equipment is kept running the store and website?
Yes **No**

Note: This room is in the back of the store in an employee-only area secured by a locked door.

Is the access to your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?
Yes **No**

Note: The computing infrastructure is in a non-public room in the back of the store secured by a door to which only certain personnel have access to.

Are visitors escorted into and out of controlled areas?
Yes **No**

Note: I was allowed to go anywhere inside the store without escort but my badge did not work on all doors.

Are there security cameras inside and outside of the store?
Yes **No**

Note: There were two cameras on the exterior of the store and 3 inside. 2 inside watch the public access part and the other is inside of the computing infrastructure room.

Is the equipment contained inside the server rack with a lock?
Yes **No**

Brandon Morgan

Sylena Beccles

Michael Varrella

Note: The equipment is inside a server rack but there is no lock on the door of the rack to get inside.

Is there a firewall in place?
Yes **No**

Note: The firewall being used could use an upgrade because it will be non-supported by Cisco soon.

Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?
Yes **No**

Note: There are some PCs located inside controlled areas but there are also some in the front of the store which could become accessible to the public.

Are screens automatically locked after 10 minutes idle?
Yes **No**

Note: This was noticed for all computers and users.

Do you have procedures for protecting data during equipment repairs?
Yes **No**

Note: They have scheduled backups but not actual procedures for when scheduled repairs are happening

Do you have an emergency evacuation plan?
Yes **No**

Note: Was last revised/created in 2020.

Does your plan identify areas and facilities that need to be sealed off immediately in case of an emergency?
Yes **No**

Note: This is not identified but all doors and areas are only accessed by authorized badges.

ACCOUNT AND PASSWORD MANAGEMENT

Brandon Morgan

Sylena Beccles

Michael Varrella

Do you have policies and standards covering electronic authentication, authorization, and access control of personnel and resources to your information systems, applications, and data?
Yes **No**

Note: These policies are put into place and enforced within the organization.

Do you ensure that only authorized personnel have access to your computers?
Yes **No**

Note: All employees have their own accounts to login to the computers.

Do you ensure that each account has the correct amount of privileges as needed to do their job?
Yes **No**

Note: All accounts have the same privilege rights on the system. Those privilege rights all seem to be administrators.

Is there a password policy?
Yes **No**

Note: The policy is not enforced.

Are your passwords secure (not easy to guess, no use of temporary or default passwords)?
Yes **No**

Note: Many are using the default or commonly known passwords for their accounts.

Are your computers set up so others cannot view staff entering passwords?
Yes **No**

Note: Is behind a counter not facing the outside of the room but there is a window behind allowing people from outside to see.

Are passwords set to expire?
Yes **No**

Note: Was told by an employee of 5 years that her password has never changed which is a big threat/risk.

CONFIDENTIALITY OF SENSITIVE DATA

Brandon Morgan

Sylena Beccles

Michael Varrella

Do you classify your data, identifying sensitive data versus non-sensitive?
Yes **No**

Note: Data is stored as either private, confidential, internal, or public.

Is the most valuable or sensitive data encrypted?
Yes **No**

Note: Everything is in clear text.

Do you have a policy for identifying the retention of information (both hard and soft copies)?
Yes **No**

Note: Some but not all.

Do you have procedures in place to deal with credit card information?
Yes **No**

Note: Staff understands the importance and their responsibility when handling credit card information.

Is there a process for creating retrievable backup and archival copies of critical information?
Yes **No**

Note: There is a database where all critical information is stored and backed up for later use.

Is there a consistent backup schedule that takes place?
Yes **No**

Note: They have a schedule to back up all their information/data every month. They then save that backup and one more before then.

Do you have procedures for disposing of waste material?
Yes **No**

Note: All unwanted documents are shredded at the end of the day.

Is waste paper shredded?
Yes **No**

Note: Everything that is waste is required to be shredded.

Brandon Morgan

Sylena Beccles

Michael Varrella

Is your shred bin locked at all times?
Yes **No**

Note: The bin itself is not locked but is stored in a secure area with authorization needed to get inside.

Do your disposal procedures identify appropriate technologies and methods for making hardware and electronic media unusable and inaccessible (such as shredding CDs and DVDs, electronically wiping drives, burning tapes), etc.)?
Yes **No**

Note: The procedure for disposing of electronic equipment is very vague and does not include everything like CDs.

DISASTER RECOVERY

Do you have a current business continuity plan?
Yes **No**

Note: Is in place and known by staff.

Is there a process for creating retrievable backup and archival copies of critical information?
Yes **No**

Note: The process is known and done regularly.

Do you have an emergency/incident management communications plan?
Yes **No**

Note: All staff members know the procedures and who to contact.

Do you have a procedure for notifying authorities in the case of a disaster or security incident?
Yes **No**

Note: All staff members know the procedures and have a contact list in the back of who to contact.

Brandon Morgan

Sylena Beccles

Michael Varrella

Does your procedure identify who should be contacted, including contact information?
Yes **No**

Note: All staff have been advised with who to contact and have a contact list in the back just in case.

Is the contact information sorted and identified by incident type?
Yes **No**

Note: All incident types are pointed to contact the same people.

Can emergency procedures be appropriately implemented, as needed, by those responsible?
Yes **No**

Note: All have been trained in proper implementation.

SECURITY AWARENESS

Are you providing information about computer security to your staff?
Yes **No**

Note: Training was provided when hired.

Do you provide training on a regular recurring basis?
Yes **No**

Note: Staff was given free online training when starting and nothing has followed.

Are employees taught to be alert to possible security breaches?
Yes **No**

Note: They were taught in their training but do not seem to be as proactive and alert as they should be.

Are your employees taught about keeping their passwords secure?
Yes **No**

Note: They know not to share it with anyone but do not handle their password information securely. (Noticed an employee go onto their phone to look up their password for the computer)

Brandon Morgan

Sylena Beccles

Michael Varrella

Does your awareness and education plan teach proper methods for managing credit card data (PCI standards) and personal private information (Social security numbers, names, addresses, phone numbers, etc.)?
Yes **No**

Note: All information is taught and required to be known before being eligible to work.

COMPLIANCE

Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?
Yes **No**

Note: When looking at their security documents the creation/revision date was 2020.

Do you audit your processes and procedures for compliance with established policies and standards?
Yes **No**

Note: Just like their security documents there has not been an audit since 2020.

Do you test your disaster plans on a regular basis?
Yes **No**

Note: Is put into place but has never been tested.

Does management regularly review lists of individuals with physical access to sensitive facilities or electronic access to information systems?
Yes **No**

Note: There are employees listed that have not been working there for over a year.

Is all IT equipment up to date with the latest updates, patches, and firmware?
Yes **No**

Note: All equipment seems to not have been updated since installation.

Template Source:
https://public-library.safetyculture.io/products/basic-risk-assessment-template?amp_dev=074a0fb7-196a-4139-bf8f-9411171f8dd1&__hstc=101368670.dbf2d49486d74f3e7d74c59b3f453fda.1727543773898.1727543773898.1727543773898.1&__hssc=101368670.3.1727543773898&__hsfp=1938985155

Brandon Morgan

Sylena Beccles

Michael Varrella

RISK ASSESSMENT

Potential Risk	Assets At Risk	Likelihood 1 = Unlikely 5 = Very Likely	Severity 1 = Little 5 = Major	Risk Factor (L x S) Low (1-8) Medium (9-14) High (15-25)	Reason	Mitigation
Hurricane	Servers hosting website Inventory Building housing servers and inventory	2	3	6	In New Jersey, there is a risk of hurricanes, and being within an hour from the coast there is a possible chance of damage to the store and the physical hardware inside.	Have a disaster recovery plan. Have Backups of all data. Have a second off-site location for all equipment needed for data storage and to keep uptime of website and store operations, that is a minimum of 90 miles away.
Retaliation of former employees	PII Trade secrets Physical security systems	3	5	15	As noticed during my checklist there were former employees still on the list as working and their accounts were never terminated. Also since all the users have the same administrative privileges on the computer a lot of harm could be done.	To mitigate this, the company should establish termination procedures that promptly revoke access to systems and deactivate accounts upon termination. Also, employees should only be given administrative privileges when necessary for their roles, that way access rights are limited to what is required.

Brandon Morgan

Sylena Beccles

Michael Varrella

Unauthorized access to employee accounts	Employee accounts Sensitive data	5	5	25	The company has many vulnerabilities that increase the risk of unauthorized access to employee accounts. The key issues include visitors not being escorted allowing unauthorized individuals access to sensitive areas. The positioning of the computers facing windows makes it easy for anyone looking in to view sensitive information. As well as, many employees use common or default passwords, making it easier for attackers to compromise accounts.	To mitigate this, the company should implement an escort policy for visitors. Also, they should relocate their computers away from windows to prevent shoulder surfing. Lastly, they need to implement a strong password policy and conduct regular security training to enhance employee awareness.
Data interception	Customer information Credit card information Trade secrets	4	5	20	Data is not encrypted when communicating across the company's systems.	To mitigate this, the company should implement IPS and DLP solutions to the company's digital ecosystem. This will detect any intruders in the company's systems and block them, and a DLP tool

Brandon Morgan

Sylena Beccles

Michael Varrella

	Employee data					will prevent any data from leaking from the system. Implementing a data encryption standard like AES-256 would help in a lot of ways.
Vulnerable to known vulnerabilities in software/hardware	Customer information Data integrity Servers	3	3	9	No one has been updating software, patches, and firmware. Automatic updates are not configured.	To mitigate this, the company should implement the usage of a threat feed and monitor the vulnerabilities in their system. Based on the information, a change management process should be implemented to patch the vulnerabilities in their systems.
Visitors tampering or harming the business inside the store	Inventory Physical security systems Price integrity Employee safety Customer safety	4	4	16	Due to the company's lack of an escort policy for visitors, the likelihood of tampering or harm is high. This could lead to significant financial losses, operational disruptions, etc.	To mitigate, the company should implement an escort policy for all visitors to ensure unauthorized individuals can't access sensitive areas.
Loss of data during repair.	PII Credit card information Customer information Employee information Inventory information	3	4	12	There is no procedure on what to do when equipment is getting repaired.	To mitigate, the company should implement a proper backup process. Having an effective backup process will allow systems to come back online and return to the same, if not almost exact, state prior to data loss. Snapshotting and journaling are effective methods.

Brandon Morgan

Sylena Beccles

Michael Varrella

Social Engineering	Confidential and Private Information Computing infrastructure Access to unauthorized areas/equipment	3	3	9	Because of their training not being enforced yearly, many employees seem to have forgotten or just do not care to notice what could be social engineering.	Require yearly training for all employees to help them identify social engineering and know how to react to it. Along with training, there should be an audit done on their own employees yearly to see if they comply with the company's standards.
Outdated policies	Customer and staff safety Data integrity Acceptable usage of equipment and data.	4	2	10	All policies have not been updated since 2020.	Update all policies and have employees acknowledge and comply with changes.
Website Outage	Customer Availability	3	2	6	Denial of service attacks. Power outage Equipment failure.	Complete patches and updates on all equipment. Upgrade firewall. Implement ACLs(Access Control Lists) Equipment redundancy

Risk Assessment Template:
https://ikase.us/project-management-risk-assessment-template/sample-45-useful-risk-register-templates-word-excel-templatelab-project-management-risk-assessment-template-pdf/