



# Cyber Security Checklist

Marketing / 11 May 2023 / John Jack Daniel

**Complete**

Score	<b>89.29%</b>	Flagged items	<b>6</b>	Actions	<b>1</b>
<b>Department</b>					Marketing
<b>Date and Time of Inspection</b>					11.05.2023 17:48 PST
<b>IT Personnel (Full Name)</b>					John Jack Daniel

## Flagged items & Actions

6 flagged, 1 action

### Flagged items

6 flagged, 1 action

Inspection / PEOPLE

#### Is a current picture part of the ID badge?

No

No picture on the ID badge



Photo 1

Inspection / 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?

No

Review visitor policies

Inspection / PHYSICAL SECURITY

#### Are there procedures in place to prevent computers from being left in a logged on state, however briefly?

No

Some employees left their PC's unlocked when they left their stations

Inspection / PHYSICAL SECURITY

#### Are screens automatically locked after 10 minutes idle?

No

Change the settings of all PC

Inspection / ACCOUNT AND PASSWORD MANAGEMENT

#### Do you require and enforce appropriate passwords?

No

To Do | Assignee SafetyCulture Staff | Priority Low | Due 18.05.2023 17:53 PST | Created by SafetyCulture Staff

Change settings for password set up

Inspection / DISASTER RECOVERY

#### Do you have a procedure for notifying authorities in the case of a disaster or security incident?

No

Review disaster recovery policies

**Other actions**

0 actions

## Inspection

6 flagged, 1 action, 89.29%

## PEOPLE

1 flagged, 83.33%

Does your staff wear ID badges?

Yes

Is a current picture part of the ID badge?

No

No picture on the ID badge



Photo 1

Are authorized access levels and type (employee, contractor, visitor) identified on the badge?

Yes

Do you check the credentials of external contractors?

Yes

Do you have policies addressing background checks for employees and contractors?

Yes

Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?

Yes

## PHYSICAL SECURITY

3 flagged, 76.92%

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?

No

Review visitor policies

Does 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

Is the access to your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?

Yes

Are visitors escorted into and out of controlled areas?

Yes

Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?

Yes

<b>Is your computing area and equipment physically secured?</b>	Yes
<b>Are there procedures in place to prevent computers from being left in a logged on state, however briefly?</b>	No
Some employees left their PC's unlocked when they left their stations	
<b>Are screens automatically locked after 10 minutes idle?</b>	No
Change the settings of all PC	
<b>Are modems set to Auto-Answer OFF (not to accept incoming calls)?</b>	N/A
<b>Do you have procedures for protecting data during equipment repairs?</b>	Yes
<b>Do you have policies covering laptop security (e.g. cable lock or secure storage)?</b>	Yes
<b>Do you have an emergency evacuation plan and is it current?</b>	Yes
<b>Does your plan identify areas and facilities that needs to be sealed off immediately in case of an emergency?</b>	Yes
<b>Are key personnel aware of which areas and facilities need to be sealed off and how?</b>	Yes

## ACCOUNT AND PASSWORD MANAGEMENT

1 flagged, 1 action, 80%

<b>Do you have policies and standards covering electronic authentication, authorization, and access control of personnel and resources to your information systems, applications and data?</b>	Yes
<b>Do you ensure that only authorized personnel have access to your computers?</b>	Yes
<b>Do you require and enforce appropriate passwords?</b>	No
To Do   Assignee SafetyCulture Staff   Priority Low   Due 18.05.2023 17:53 PST   Created by SafetyCulture Staff	
Change settings for password set up	
<b>Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?</b>	Yes
<b>Are your computers set up so others cannot view staff entering passwords?</b>	Yes

## CONFIDENTIALITY OF SENSITIVE DATA

100%

Do you classify your data, identifying sensitive data versus non sensitive?	Yes
Are you exercising responsibilities to protect sensitive data under your control?	Yes
Is the most valuable or sensitive data encrypted?	Yes
Do you have a policy for identifying the retention of information (both hard and soft copies)?	Yes
Do you have procedures in place to deal with credit card information?	Yes
Do you have procedures covering the management of personal private information?	Yes
Is there a process for creating retrievable back up and archival copies of critical information?	Yes
Do you have procedures for disposing of waste material?	Yes
Is waste paper binned or shredded?	Yes
Is your shred bin locked at all times?	Yes
Do your policies for disposing of old computer equipment protect against loss of data (e.g. by reading old disks and hard drives)?	Yes
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

## DISASTER RECOVERY

1 flagged, 90%

Do you have a current business continuity plan?	Yes
Is there a process for creating retrievable back up and archival copies of critical information?	Yes
Do you have an emergency/incident management communications plan?	Yes
Do you have a procedure for notifying authorities in the case of a disaster or security incident?	No

[Review disaster recovery policies](#)

Does your procedure identify who should be contacted, including contact information?	Yes
Is the contact information sorted and identified by incident type?	Yes
Does your procedure identify who should make the contacts?	Yes
Have you identified who will speak to the press/public in the case of an emergency or an incident?	Yes
Does your communications plan cover internal communications with your employees and their families?	Yes
Can emergency procedures be appropriately implemented, as needed, by those responsible?	Yes

## SECURITY AWARENESS

100%

Are you providing information about computer security to your staff?	Yes
Do you provide training on a regular recurring basis?	Yes
Are employees taught to be alert to possible security breaches?	Yes
Are your employees taught about keeping their passwords secure?	Yes
Are your employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?	Yes
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

## COMPLIANCE

100%

Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?	Yes
Set a meeting with Carl to review security policies	
Do you audit your processes and procedures for compliance with established policies and standards?	Yes
Do you test your disaster plans on a regular basis?	Yes

**Does management regularly review lists of individuals with physical access to sensitive facilities or electronic access to information systems?**

Yes

---

## COMPLETION

---

### Overall Recommendations

- Replace ID badges with employee photos
  - Review security and disaster policies
  - Conduct employee training about cyber security policies
  - Change password settings (require complex password)
- 

### IT Personnel (Name and Signature)



John Jack Daniel  
11.05.2023 17:55 PST

---



## Media summary



Photo 1