Marketing / 03 Sep 2019 / John Jack Daniel

Cyber Security Checklist

Complete

Inspection score	Failed items	Created actions
89.29%	6	4

Department Marketing
Date and Time of Inspection 3rd Sep, 2019 9:17 AM +08
IT Personnel (Full Name) John Jack Daniel

Failed items

6 Failed

Inspection / PEOPLE

Is a current picture part of the ID badge?	No

— Notes

No picture on the ID badge

— Photos

Photo 1

— Actions

To Do **Replace ID badge with current picture**

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

— Notes

Review visitor policies

Are there procedures in place to prevent computers from being left in a loggedon state, however briefly?	No

— Notes

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

Are screens automatically locked after 10 minutes idle?	No

— Notes

Change the settings of all PC

— Actions

To Do **Change settings of all PC in Marketing Dept**

Inspection / ACCOUNT AND PASSWORD MANAGEMENT

Do you require and enforce appropriate passwords?	No

— Notes

Change settings for password set up

— Actions

To Do **Implement strong password setting**

Inspection / DISASTER RECOVERY

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

— Notes

Review disaster recovery policies

— Actions

To Do **Review disaster policies**

Actions

4 Actions

created a High priority action

To Do 4th Sep, 2019 8:00 AM +08

Review disaster policies

Inspection / DISASTER RECOVERY

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

created a High priority action

To Do 3rd Sep, 2019 8:00 AM +08

Implement strong password setting

Inspection / ACCOUNT AND PASSWORD MANAGEMENT

Do you require and enforce appropriate passwords?

created a High priority action

To Do 3rd Sep, 2019 8:00 AM +08

Change settings of all PC in Marketing Dept

Inspection / PHYSICAL SECURITY

Are screens automatically locked after 10 minutes idle?

created a High priority action

To Do 4th Oct, 2019 8:00 AM +08

Replace ID badge with current picture

Inspection / PEOPLE

Is a current picture part of the ID badge?

Inspection

6 Failed 4 Actions 89.29%

PEOPLE

1 Failed 1 Action

Does your staff wear ID badges?	Yes
Is a current picture part of the ID badge?	No

— Notes

No picture on the ID badge

— Photos

Photo 1

— Actions

To Do **Replace ID badge with current picture**

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 Failed 1 Action

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

— Notes

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
Is your computing area and equipment physically secured?	Yes
Are there procedures in place to prevent computers from being left in a loggedon state, however briefly?	No

— Notes

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

Are screens automatically locked after 10 minutes idle?	No

— Notes

Change the settings of all PC

— Actions

To Do **Change settings of all PC in Marketing Dept**

Are modems set to Auto-Answer OFF (not to accept incoming calls)?	N/A
Do you have procedures for protecting data during equipment repairs?	Yes
Do you have policies covering laptop security (e.g. cable lock or secure storage)?	Yes
Do you have an emergency evacuation plan and is it current?	Yes
Does your plan identify areas and facilities that needs to be sealed off immediately in case of an emergency?	Yes
Are key personnel aware of which areas and facilities need to be sealed off and how?	Yes

ACCOUNT AND PASSWORD MANAGEMENT

1 Failed 1 Action

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
Do you ensure that only authorized personnel have access to your computers?	Yes
Do you require and enforce appropriate passwords?	No

— Notes

Change settings for password set up

— Actions

To Do **Implement strong password setting**

Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?	Yes
Are your computers set up so others cannot view staff entering passwords?	Yes

CONFIDENTIALITY OF SENSITIVE DATA

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 Failed 1 Action

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
— Notes Review disaster recovery policies — Actions To Do **Review disaster 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

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

Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?	Yes
— Notes 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

3rd Sep, 2019 10:11 AM +08

Photos

1 Photos

Photo 1