



IT Risk Assessment Template

conducted for

East Coast Data Center

Conducted on

04 Jan 2019 01:26 PM

Prepared by

Justine J.

Completed on

04 Jan 2019 02:26 PM

Score

0/0.0 - 0.00%

Failed Responses

This section lists responses that were set as "failed responses" in the template used for this audit

Question	Response	Details
Risk rating	High	

Actions

#1. Hello Anne, I'll drop by before end of shift today. Kindly read the new directive on information security sent out last month. Thanks!

Assignee: anne.karin.admin@safetyculture.com
Priority: LOW
Due Date: 04 Jan 2019 04:00 PM
Audit: 04 Jan 2019 / East Coast Data Center / Justine J.
Linked to item: Recommended controls or alternative options for reducing risk
Status: To Do


#2. Hello Dan and Trevor, It has come to my attention that a laptop issued last month wasn't set with the default password. I'll meet with you before end of shift today to reinforce the importance of security. You are well aware that we are working towards ISO 27001 certification. Thank you!



Assignee: east.it.team@safetyculture.com
Priority: HIGH
Due Date: 04 Jan 2019 05:00 PM
Audit: 04 Jan 2019 / East Coast Data Center / Justine J.
Linked to item: Recommended controls or alternative options for reducing risk
Status: To Do



#3. Hello Anne, Please call our vendor to fix the magnetic lock of our east exit if you haven't contacted them yet. I don't have their phone # or email with me. Thank you!

Assignee: anne.karin.admin@safetyculture.com
Priority: HIGH
Due Date: -
Audit: 04 Jan 2019 / East Coast Data Center / Justine J.
Linked to item: Recommended controls or alternative options for reducing risk
Status: To Do

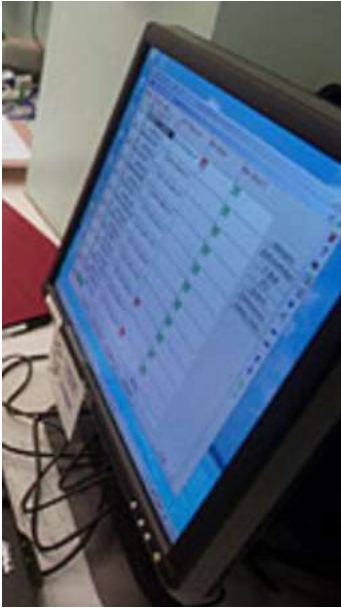
Audit

Question	Response	Details
General		
Describe the purpose of this IT security risk assessment	To assess current information security risks	
Describe the scope of the risk assessment	East Coast facility	
List all participants including role (e.g. system owner, system custodian, network manager etc.)	Head of IT Facility Manager	
Describe key technology components including commercial software	Desktops, Laptops, Server Room, proprietary software	
Describe how users access the system and their intended use of the system	staff access the system by logging in to their designated desktops, management have their designated laptops	
Risk Assessment		
Click Add Vulnerability (+) after you have identified a vulnerability or threat source		
Vulnerability 1		
Threat Source & Vulnerability		
Observation	Reception desktop left unlocked	
Threat source/ vulnerability	Intentional Insider	
Evidence (flow diagrams, screenshots etc.) (optional)		
		
Appendix 1		
Existing controls	Guard near the door CCTV	
Risk rating		
Consequence	Medium	
Likelihood	Unlikely	

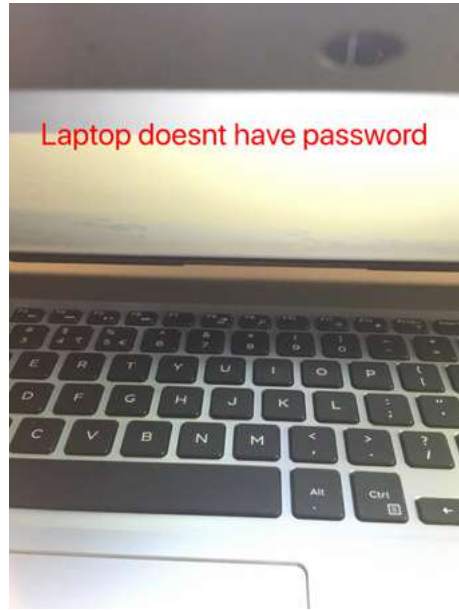
Question	Response	Details
Risk rating	Medium	
Recommended Controls		
Recommended controls or alternative options for reducing risk	Reinforce the importance of locking the PC when not in use. I will talk to Anne and remind her of our directive to improve our information security for ISO 27001 certification.	
Vulnerability 2		
Threat Source & Vulnerability		
Observation	Laptop doesn't have password set	
Threat source/ vulnerability	Intentional Outsider	
Evidence (flow diagrams, screenshots etc.) (optional)		
<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>Appendix 2</p> </div> <div style="text-align: center;">  <p>Appendix 3</p> </div> </div>		
Existing controls	This was a laptop issued last month and should already have the default password before it was handed to the new staff.	
Risk rating		
Consequence	High	
Likelihood	Likely	
Risk rating	High	
Recommended Controls		
Recommended controls or alternative options for reducing risk	Will meet with Dan H. who issued the new laptop and his supervisor Trevor N. Will advise about a possible warning.	
Vulnerability 3		
Threat Source & Vulnerability		
Observation	east exit's newly installed glass door magnetic locks are malfunctioning	

Question	Response	Details	
Threat source/ vulnerability	Intentional Outsider		
Evidence (flow diagrams, screenshots etc.) (optional)			
 <p data-bbox="140 539 256 566">Appendix 4</p>			
Existing controls	Guard by the door and CCTV		
Risk rating			
Consequence	High		
Likelihood	Unlikely		
Risk rating	Medium		
Recommended Controls			
Recommended controls or alternative options for reducing risk	Facilities need to fix the magnetic lock. Exit will guarded 24/7 but we will not allow access to this door until this is fixed.		
Completion			
Recommendations	Majority of staff are still on holiday vacation but we found plenty of security risks today. Will conduct a meeting when everybody's back next week to reinforce the directive to get our ISO 27001 certification.		
Signature	Justine J.	04 Jan 2019 02:26 PM	

Media



Appendix 1



Appendix 2



Appendix 3



Appendix 4