SC

IT Risk Assessment Template

10 Apr 2023 / East Coast Data Center / Justine J.   **Complete**

Score	0%	Flagged items	1	Actions	0

Conducted on	10.04.2023 10:30 PST

System Owner	East Coast Data Center

Prepared by	Justine J.

Audit / Risk Assessment / Vulnerability / Vulnerability 2 / Risk rating

Risk rating

High

Audit	1 flagged

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   1 flagged

Click Add Vulnerability (+) after you have identified a vulnerability or threat source

Vulnerability   1 flagged

Vulnerability 1

Threat Source & Vulnerability

Observation

Reception desktop left unlocked

Threat source/ vulnerability	Intentional Insider

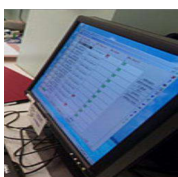**Evidence (flow diagrams, screenshots etc.) (optional)**

Photo 1

Existing controls

Guard near the door
CCTV

Risk rating

Consequence	Medium
Likelihood	Unlikely
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   1 flagged

Threat Source & Vulnerability

Observation

Laptop doesn't have password set

Threat source/ vulnerability	Intentional Outsider

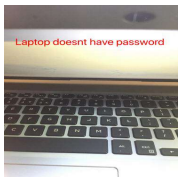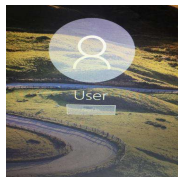### Evidence (flow diagrams, screenshots etc.) (optional)

Photo 2

Photo 3

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   1 flagged

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

Threat source/ vulnerability	Intentional Outsider

Evidence (flow diagrams, screenshots etc.) (optional)

Photo 4

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.
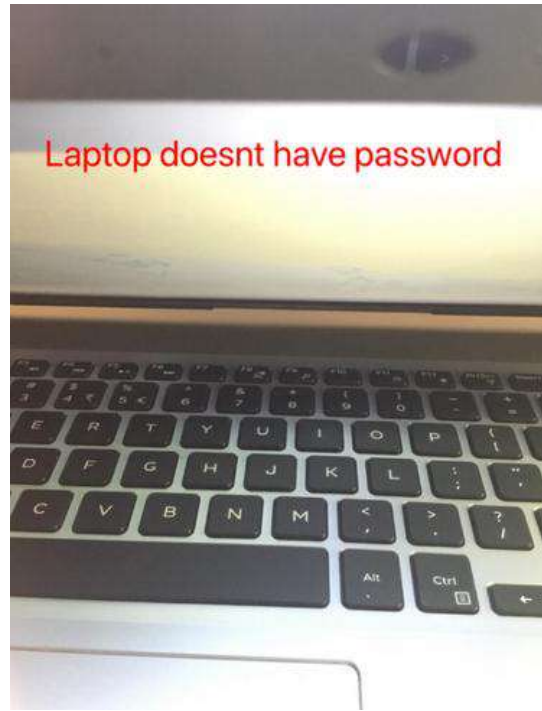
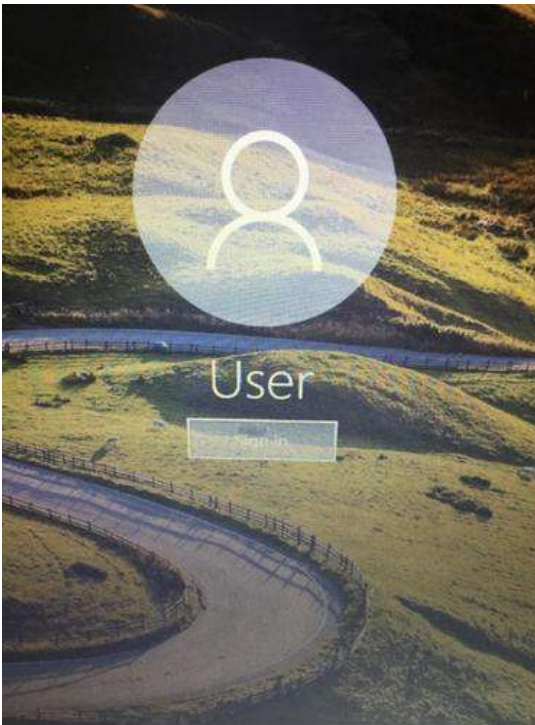## Signature

Justine J.
10.04.2023 11:00 PST

Photo 1

Laptop doesnt have password

Photo 2

User

Photo 3

EXIT

Photo 4