Cybersecurity Risk Assessment for Laboratory

This deliverable is made to cover the who, what, and when situations at the laboratory. The “who” is the demographic that is affected by the cybersecurity/tech hazards at the lab and who needs to resolve said hazard. The “what” are the hazards, mitigation techniques, and mitigation techniques after the incident. The “when” are time slots to when the mitigation techniques should be implemented for the laboratory. It is supposed to be a document that the manager or anyone apart from the it can use as a reference to when a situation occurs.

By: Roger Asquith and Robert Fleek

What are the hazards?	Who might be harmed and how?	What are you already doing to control the risks?	What further action do you need to take to control the risks?	Who needs to carry out the action?	When is the action needed by?	Done
Data loss	Employees at Maranyane Medical Laboratory	Saving information on the cloud or on a physical disk	Continue to do backups.	Manager	At the end of every month	(Insert the day before the end of the month)
Weak passwords	Employees at Maranyane Medical Laboratory	Requiring employees to have passwords that are 12 characters, including symbols, and capital lettering	Change passwords every year	Manager	At the end of every year.	(Insert the day before the end of the month)
Unauthorized Device Acess	Employees at Maranyane Medical Laboratory	Requiring employees to use pre-approved devices for lab	Checking the types of devices that are connected to the network	?	Every single week or at the end of the month.	(Insert the day before the end of the month)

		work				
Insecure Network Connections	Employees at Maranyane Medical Laboratory	Establish firewalls through a 3rd party service or use Windows firewall service	Find a 3rd party firewall service or enable Windows firewall on all devices	Manager	At the end of the week after 3rd party software is found.	(Insert the day before the end of the month)
Cybersecurity Training	Employees at Maranyane Medical Laboratory	There's no training for employees	Create deliveries exploring cybersecurity concepts	Manager	End of the month	(Insert the day before the end of the month)
Phishing Attacks	Employees at Maranyane Medical Laboratory	There is no training for employees	Create deliveries explaining how Phishing works and how to prevent it	Manager	End of the month	(Insert the day before the end of the month)
Insider threats	Employees at Maranyane Medical Laboratory	There is no training for employees	Create deliveries explaining what Insider threats are and how to prevent them	Manager	End of the month	(Insert the day before the end of the month)

Unpatched Software	Employees at Maranyane Medical Laboratory	There's minimal training	Create delivered on how to update software	Manager	End of the month	(Insert the day before the end of the month)
Data Theft and Espionage	Employees at Maranyane Medical Laboratory	There's minimal training	Explaining	Manager	End of the month	(Insert the day before the end of the month)
Inadequate Physical Security	Employees at Maranyane Medical Laboratory	Assess the use of locks, surveillance cameras, and visitor logs.	Install access control systems, like keycards or biometric locks, and train employees on securing sensitive physical documents.	Manager	Within three months	(Insert the day before the end of the month)
Lack of antivirus and anti-malware software on lab computers.	can corrupt data or compromise systems.	Use built-in OS protections if available.	Install reliable antivirus software on all computers and ensure it's regularly updated.	IT Specialist or Manager	Immediate	(Insert the day before the end of the month)

Sensitive data not encrypted.	Loss or theft of data due to unauthorized access.	None specified.	Implement encryption for both data at rest (stored) and data in transit (during transfer).	Manager	End of the month	(Insert the day before the end of the month)
Employees using personal devices for lab-related work.	data leaks or malware infections if devices are not secure.	Not specified.	Enforce a strict BYOD policy, restricting access to lab systems or requiring additional security checks on personal devices.	IT Specialist or Manager	End of the month	(Insert the day before the end of the month)
Lack of secure procedures for remote access (if applicable).	Increased risk of unauthorized access and data leaks	Use VPN or secure connection protocols.	Implement a VPN for remote access and educate staff on remote work best practices.	IT Specialist	Within two weeks	(Insert the day before the end of the month)