



# IT3070 Information Assurance & Security

## 3<sup>rd</sup> Year 1<sup>st</sup> Semester - 2025

Sri Lanka Institute Of Nanotechnology  
(SLINTECH)

### Team Members

Student ID	Student Name	Selected Asset
IT231913	Dissanayaka P.G.J.S	Research Data
IT232879	Gunasekara T	Central Server
IT234048	Thennakoon T.M.R.T	Network infrastructure

## Table of Contents

Introduction.....	2
Assets .....	3
Risk to the assets.....	3
1. IT234048.....	4
Network Infrastructure.....	4
2. IT231913.....	14
Research Data .....	14
3. IT232879.....	24
Central Server .....	24
References.....	33

## Introduction

The Sri Lanka Institute of nanotechnology (Commonly known as SLINTEC) Is a institute specializing in field of nanotechnology. It was incorporated in 2008 as a public- private partnership between government of Sri Lanka and five private companies and is notable for being the first public-private research institute seeking to promote nanotechnology research in Sri Lanka. The initiative cited several other related objectives.

- Developing nanotechnology-based industry
- Attracting nanotechnology expertise to Sri Lanka
- Increase the competitiveness of local industry through local R&D
- Value addition to national resources and export

Main research focus areas are,

Agriculture - Nonfertilizer, insecticides and pesticides, nutrient systems

Apparel – Nano fabrics, smart fabrics

Energy – nanotechnology solutions for efficient energy storage and generation

Advanced materials

Healthcare – nutraceuticals, natural products [1]

SLINTEC's achievements, such as securing a \$2.2M patent for slow- release nano fertilizer and forming strategic partnerships with industry leaders like Brandix and MAS holdings.

## Assets

1. Network infrastructure
2. Central Server
3. Database
4. Hospital System
5. Research Data / Patient

## Risk to the assets

1. Network infrastructure
  - DDOS Attack
  - Firmware Exploit
2. Research Data
  - SQL Injection
  - Data Breach
3. Server
  - Environmental and physical hazards (Fire, Power short)
  - Exploitation of unpatched vulnerabilities in server

# 1. IT234048

## Network Infrastructure

<b>Allegro Worksheet 8</b>			<b>CRITICAL INFORMATION ASSET PROFILE</b>
<b>(1) Critical Asset</b> <i>What is the critical information asset?</i>	<b>(2) Rationale for Selection</b> <i>Why is this information asset important to the organization?</i>	<b>(3) Description</b> <i>What is the agreed-upon description of this information asset?</i>	
Network Infrastructure	Since it connects all research systems, administrative servers, and users, the network infrastructure is essential to SLINTEC. It facilitates secure data sharing, communication, and cloud service access for research teams. Key operations such as email communication, data transfer, and research database access would not be possible without it.	All users and systems within SLINTEC are connected by the network infrastructure, which consists of servers, routers, switches, firewalls, access points, and cables. It enables safe communication with cloud services and research partners and offers both wired and wireless connections within the organization. It manages data communication between administrative platforms, research servers, and staff devices, ensuring that each department's network stays separated to maintain high security and effectiveness.	
<b>(4) Owner(s)</b> <i>Who owns this information asset?</i>			
Head – IT Division (Network Administrator)			
<b>(5) Security Requirements</b> <i>What are the security requirements for this information asset?</i>			
<input type="checkbox"/> <b>Confidentiality</b>	Only authorized personnel can view this information asset, as follows:	Networking devices such as servers, routers, and firewalls should only be accessible by authorized IT personnel. System logs, network credentials, and sensitive configurations should not be revealed to regular employees and outsiders. Network devices must be accessed using role-based access control and protected using strong authentication procedures.	

<input type="checkbox"/> <b>Integrity</b>	Only authorized personnel can modify this information asset, as follows:	Only the network administrators can modify network settings, install firmware updates, or modify security policies. Security vulnerabilities or loss of service results from any unauthorized modification. To maintain integrity, change management processes and configuration backups must be followed.
<input type="checkbox"/> <b>Availability</b>	This asset must be available for these personnel to do their jobs, as follows:	
<input type="checkbox"/> <b>Other</b>	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	Authorized personnel must have access to network infrastructure in order to support ongoing administrative activities, communication, and research projects. Researchers, employees, and operational systems may be affected by network device failures or disruptions. Network connectivity must be available twenty-four hours a day, seven days a week, fifty-two weeks a year, with extra network devices and automatic switching systems and backups in place to avoid service interruptions.
<input type="checkbox"/> <b>Other</b>	This asset has special regulatory compliance protection requirements, as follows:	To ensure secure communication and data transfer across all departments, the network must comply with SLINTEC's internal IT security policy and national data protection standards.

#### (6) Most Important Security Requirement

*What is the most important security requirement for this information asset?*

<input type="checkbox"/> Confidentiality	<input type="checkbox"/> Integrity	<input checked="" type="checkbox"/> Availability	<input type="checkbox"/> Other
--	------------------------------------	--	--------------------------------

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Network Infrastructure		
		Area of Concern	Distributed Denial of Service (DDoS) Attack		
		(1) Actor <i>Who would exploit the area of concern or threat?</i>	Hacker		
		(2) Means <i>How would the actor do it? What would they do?</i>	SLINTEC's network devices such as routers, switches, and firewalls can be slowed down by massive traffic, making the system unavailable to authorized staff in a distributed denial of service (DDoS) attack. In a DDoS attack, the attacker makes use of a botnet or public services like DNS or NTP to flood SLINTEC's network. The attack sends an extremely high amount of traffic to SLINTEC's network devices, including web servers, routers, and firewalls. This saturates the network and devices, making services unavailable to authorized personnel. Attackers can also use IP spoofing or other methods of evading simple filtering, and no authorized account or internal access is required to launch the attack.		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Deliberate		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input checked="" type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	A DDoS attack primarily targets the availability of SLINTEC's network infrastructure. Flooding the network with too much traffic overloads the bandwidth and its devices, making critical services unavailable to authorized personnel. Integrity may be violated, when IT staff rushingly apply network configuration changes during the attack, that might unintentionally introduce errors or incorrect configurations. Confidentiality is not affected directly by DDoS attacks, but attackers may take advantage of the disruption as an opportunity to attempt to engage in further unauthorized activities. Overall, DDoS attacks primarily violate <b>availability</b> ,		
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <b>75%</b> <b>50%</b> <b>25%</b>		

	(7) Consequences  <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity  <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
		Impact Area	Value	Score
DDoS attacks can disrupt SLINTEC's network infrastructure, which can seriously harm the institute's reputation. If network services become unavailable, SLINTEC may be unable to continue research, administrative operations, or communications, causing partners, collaborators, and funding agencies to lose confidence.	When a DDoS attack occurs, it takes a considerable amount of money and time to recover. SLINTEC may also need to invest in additional network security tools and services to prevent future attacks.	Reputation & Customer Confidence	8	6.0
		Financial	6	4.5
When the network infrastructure is attacked, the entire institute may be impacted, and all operations may be disrupted. Network services will experience downtime, and productivity will be decreased as a result. [2]	The attack itself may not cause legal action, but if downtime leads to non-compliance with data-sharing or service-level agreements, SLINTEC may face minor penalties.	Productivity	7	5.25
		Safety & Health	0	0
Disruptions to research activities may damage SLINTEC's standing as a reliable research institute in Sri Lanka. This could affect future collaborations or grants.	Disruptions to research activities may damage SLINTEC's standing as a reliable research institute in Sri Lanka. This could affect future collaborations or grants.	Fines & Legal Penalties	2	1.5
		User Defined Impact Area	3	2.25
				<b>Relative Risk Score      19.5</b>

### (9) Risk Mitigation

Based on the total score for this risk, what action will you take?

 Accept

 Defer

 Mitigate

 Transfer

For the risks that you decide to mitigate, perform the following:

<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>
Expand the bandwidth	SLINTEC can handle sudden increases in traffic by expanding network bandwidth. IT personnel keep an eye on the network and approve any changes that occur. Secure server locations and backup network paths are also configured. The network may still be slightly slowed by very large attacks, but essential work can continue.
Using cloud DDoS services	By blocking bad traffic before it reaches the institute, cloud-based DDoS services help SLINTEC to protect its network. IT personnel monitor network traffic and work with the cloud provider to comply with security regulations. Physical security at the provider's data centers adds an extra layer of protection. Large-scale attacks may still cause minor delays, but critical services and research projects continue uninterrupted.
Rate limiting	Limiting the number of requests a server will handle over some time period is also utilized to prevent denial-of-service attacks. Although rate limiting will be beneficial in slowing down web scrapers scraping material and for preventing brute force login, it will likely not be sufficient alone to handle a well-planned DDoS attack. [3]
Blackhole routing	One option open to nearly any network administrator is to create a blackhole route and send traffic into the route. In its most basic form, when blackhole filtering is activated without qualification restriction criteria, valid and malicious network traffic is routed to a null route, or blackhole, and removed from the network. If a website, which is an Internet property, is being DDoS-attacked, the ISP of the property will forward all traffic from the site into a blackhole as a countermeasure. This is not the ideal solution, as this actually gives the attacker their own desired outcome: it renders the network out of bounds. [4]
Extra network infrastructure	To control traffic, SLINTEC makes use of load balancers, backup servers, and additional network paths. Technical tools manage traffic distribution, and IT personnel keep an eye on and maintain these backups. Backup servers are kept in a safe location. Critical services continue to function even though large attacks may still cause slight delays.
	<p>Residual risks accepted.</p> <p>The network might still slow down during an attack.</p> <p>Some attack traffic might pass through even after applying controls.</p> <p>The response to a large attack might be slightly delayed.</p>

Attribute	Value	Justification
Probability	75%	Probability is high because there are many DDoS attacks around and the cost for initiating this type of attack is very low. One person can control botnets and completely breaks a system temporarily.
Reputation & Customer Confidence	8	A DDoS attack can disrupt SLINTEC's network services, making important systems unavailable. Researchers, staff, and collaborators may lose confidence in the institute's ability to maintain reliable operations and secure network resources. Therefore, a very high impact value is given (8/10).
Financial	6	Recovering from a DDoS attack requires significant time and money. SLINTEC may need to invest in additional network security tools and services to prevent future attacks. Therefore, a medium-to-high impact value is given (6/10).
Productivity	7	DDoS attack-induced network disruptions can stop administrative and research activities, delaying reporting, experiments, and communications. As a result, productivity is significantly affected. Therefore, a high impact value is given (7/10).
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10).
Fines & Legal Penalties	2	Although a DDoS attack may briefly disrupt services, there is minimal legal risk because no sensitive data is exposed. Therefore, a low impact value is given (2/10).
User Defined Impact Area	3	Delays in research activities caused by a DDoS attack may affect SLINTEC's credibility and slightly impact future collaborations or grant opportunities. Therefore, a medium-to-low impact value is given (3/10).

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET						
Information Asset Risk	Information Asset	Network Infrastructure						
		Firmware Exploit						
	(1) Actor <i>Who would exploit the area of concern or threat?</i>		Malicious outsider					
	(2) Means <i>How would the actor do it? What would they do?</i>		The attacker targets the firmware of network devices. They could take advantage of known vulnerabilities in outdated firmware versions by connecting to the devices through a network, web interfaces, VPNs, or other management portals. Once a device has been exploited, attackers can change the firmware, add malicious code, or prevent the device from functioning. If vulnerabilities are left unpatched, no authorized account is required.					
	(3) Motive <i>What is the actor's reason for doing it?</i>		Deliberate					
	(4) Outcome <i>What would be the resulting effect on the information asset?</i>		<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input checked="" type="checkbox"/> Modification <input type="checkbox"/> Interruption					
	(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>		A firmware exploit mainly affects the <b>integrity</b> of SLINTEC's network infrastructure. By exploiting outdated or weak firmware, attackers can install malicious code or change device settings, causing improper operations. If hackers use the exploit to gain access to or steal private information kept on devices, confidentiality may also be impacted. If modified firmware results in system errors, crashes, or network device failures, availability may be decreased. But overall, firmware exploits mainly violate <b>integrity</b> .					
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>		<input type="checkbox"/> High 75%	<input checked="" type="checkbox"/> Medium 50%	<input type="checkbox"/> Low 25%			
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>			(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>				
			<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Impact Area</th><th style="text-align: center;">Value</th><th style="text-align: center;">Score</th></tr> </thead> </table>		Impact Area	Value	Score	
Impact Area	Value	Score						

<p>A firmware exploit on SLINTEC's network devices could damage the institute's reputation. Partners and collaborators may lose trust in the integrity of research data and communications, reducing confidence in SLINTEC's ability to secure sensitive information.</p> <p>A firmware exploit could cost SLINTEC significant money and resources to recover. The institute may need to replace or reflash affected devices, restore research data integrity, and invest in improved firmware security measures, resulting in substantial financial impact.</p> <p>If network infrastructure is affected, research and administrative operations may be disrupted. Device downtime can slow communication, data transfers, and research progress, lowering overall productivity.</p> <p>If damaged devices or changed logs cause problems with data accuracy or break data protection rules, SLINTEC could face fines or legal penalties. The risk is moderate, so the potential legal impact is limited.</p> <p>Disruptions to research activities may damage SLINTEC's standing as a reliable research institute in Sri Lanka. This could affect future collaborations or grants.</p>	Reputation & Customer Confidence	9	4.5
	Financial	6	3.0
	Productivity	7	3.5
	Safety & Health	0	0
	Fines & Legal Penalties	3	1.5
	User Defined Impact Area	3	1.5
<b>Relative Risk Score</b>			<b>14.0</b>

### (9) Risk Mitigation

*Based on the total score for this risk, what action will you take?*

<input type="checkbox"/> Accept	<input type="checkbox"/> Defer	<input checked="" type="checkbox"/> Mitigate	<input type="checkbox"/> Transfer
---------------------------------	--------------------------------	--	-----------------------------------

**For the risks that you decide to mitigate, perform the following:**

On what container would you apply controls?	What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?
Administrative Access	Make use of multi-factor authentication, create secure passwords, and restrict admin account access to those who are authorized. Maintain a log of every admin action. If insiders abuse their access or if passwords are stolen, some unauthorized access may still occur.

Device Firmware	Keep all network devices with secure firmware. Test every firmware upgrade in a safe environment before installing and verify its digital signature. Devices can still be open to malicious or unknown vulnerabilities, though.
Monitoring and Early Warning	Watch device logs and network traffic for unusual activity or signs of firmware tampering. This lets IT personnel respond quickly, but some attacks might still go unnoticed for a short time.
	<p>Residual risks accepted.</p> <p>Staff might make mistakes or wrongly configure a device.</p> <p>Undetected firmware vulnerabilities.</p> <p>The system may not notice all small changes made to the device firmware.</p>

Attribute	Value	Justification
Probability	50%	Firmware exploits are possible when devices are not promptly patched or properly managed. They require some skill but are realistic for organizations with many network devices.
Reputation & Customer Confidence	9	A firmware exploit that impacts SLINTEC's network infrastructure could harm the institute's reputation. Partners and stakeholders would become less confident in SLINTEC's ability to protect sensitive data if devices were altered, which would reduce trust in research data and communications. Therefore, a very high impact value is given (9/10). [5]
Financial	6	Recovering from a firmware exploit requires significant time and money. SLINTEC may need to replace or reflash affected devices, restore data integrity, hire specialists, and invest in improved firmware security. Therefore, a medium-to-high impact value is given (6/10).
Productivity	7	Normal administrative and research activities may be disrupted. Until systems are restored, staff and researchers may face delays in communications, data transfers, research, and

		reporting. Therefore, a high impact value is given (7/10).
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10).
Fines & Legal Penalties	3	If damaged devices or altered logs lead to data accuracy failures or violations of data-protection requirements, SLINTEC may incur regulatory fines or contractual penalties. The likelihood and scale of such penalties are limited. Therefore, a medium-low legal impact value is given (3/10). [6]
User Defined Impact Area	3	Delays in research activities caused by a DDoS attack may affect SLINTEC's credibility and slightly impact future collaborations or grant opportunities. Therefore, a medium-to-low impact value is given (3/10).

## 2. IT231913

### Research Data

<b>Allegro Worksheet 8</b>			<b>CRITICAL INFORMATION ASSET PROFILE</b>
<b>(1) Critical Asset</b> <i>What is the critical information asset?</i>	<b>(2) Rationale for Selection</b> <i>Why is this information asset important to the organization?</i>	<b>(3) Description</b> <i>What is the agreed-upon description of this information asset?</i>	
Research Data	Research Data is an essential and critical asset for SLINTECH, because it contains intellectual property, Experimental Results, and sensitive information essential for the ongoing research & development, innovations, and organizational competitiveness.	SLINTECH Research Data information assets include digital essential and sensitive datasets, as well as experimental results generated during R&D. It will support scientists in their research projects, analysis, publications, and technology development. The asset also contains processed data, models, and intellectual property essential to SLINTECH's innovation and competitive position.	
<b>(4) Owner(s)</b> <i>Who owns this information asset?</i>			
Head Of Research & Development			
<b>(5) Security Requirements</b> <i>What are the security requirements for this information asset?</i>			
<input type="checkbox"/> <b>Confidentiality</b>	Only authorized personnel can view this information asset, as follows:	Research Project Data, Research processed data, models, and intellectual property must be protected from unauthorized access by anyone outside the research team or staff without proper permission.	
<input type="checkbox"/> <b>Integrity</b>	Only authorized personnel can modify this information asset, as follows:	Only authorized personnel with appropriate privileges can modify experimental results, models, and ensure accurate, complete, and sensitive information. All changes must be tracked and auditable.	
<input type="checkbox"/> <b>Availability</b>	This asset must be available for these personnel to do their jobs, as follows:		

	This asset must be available for <u>20</u> hours, <u>6</u> days/week, <u>46</u> weeks/year.	Research data must be available to authorized personnel to support ongoing research Projects, analysis, and publications. Downtime or disruptions to web servers can negatively impact Researchers and scientists. The database must be accessible during their working hours (8:00 AM - 6:00 PM) and days, with backups in place to prevent disruption.
<input type="checkbox"/> Other	This asset has special regulatory compliance protection requirements, as follows:	Compliance with ISO/IEC 17025:2017 lab accreditation [7], Sri Lanka's Data protection act(no 9 of 2022) [8]

#### (6) Most Important Security Requirement

*What is the most important security requirement for this information asset?*

<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> <b>Integrity</b>	<input type="checkbox"/> Availability	<input type="checkbox"/> Other
--	--	---------------------------------------	--------------------------------

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	Research Data
		Area of Concern	<i>Data Breach</i>
		(1) Actor <i>Who would exploit the area of concern or threat?</i>	Insider (Staff Member)
		(2) Means <i>How would the actor do it? What would they do?</i>	The internal staff member in the SLINTECH who has access to confidential research data in the system. Intentionally stole sensitive research files and data from the database. Sell that stolen, important, and sensitive research data to the outsiders who are looking for that advanced and sensitive information.
		(3) Motive <i>What is the actor's reason for doing it?</i>	Intentionally

	<p>(4) Outcome <i>What would be the resulting effect on the information asset?</i></p> <p>(5) Security Requirements <i>How would the information asset's security requirements be breached?</i></p> <p>(6) Probability <i>What is the likelihood that this threat scenario could occur?</i></p>	<input checked="" type="checkbox"/> <b>Disclosure</b> <input type="checkbox"/> <b>Destruction</b> <input type="checkbox"/> <b>Modification</b> <input type="checkbox"/> <b>Interruption</b>																							
		<p>Ensure that sensitive data of research is accessible to authorized persons (researchers and system administrators) who might require it. The data must not be shared with third parties without a legal requirement or agreement. Sensitive &amp; confidential Research data, in the wrong hands, can cause serious damage to financial reputation and loss of intellectual property to SLINTECH.</p>																							
		<input checked="" type="checkbox"/> <b>High</b> <span style="color: red;"><b>75%</b></span>	<input type="checkbox"/> <b>Medium</b> <span style="color: blue;">50%</span>	<input type="checkbox"/> <b>Low</b> <span style="color: green;">25%</span>																					
	<p>(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i></p> <p>Sensitive Research data exposed to a third party damages the SLINTECH reputation and may also lose trust among researchers, funding agencies, collaborators, participants, and international collaborators. [9]</p> <p>As a result, the Organisation's financial status will decline, and it will have to spend a significant sum of money to investigate this problem. [10]</p> <p>Causing delays in ongoing research projects and operations. Also, the research team may be disrupted due to the investigation and rework. It also may lead to employee layoffs. As a result, productivity will decline along with falling revenue. [11]</p> <p>The Research Center (SLINTECH) can lead to significant fines and legal penalties. SLINTECH could face loss of international research accreditation. These reasons will impact ongoing projects and future partnerships. [11]</p> <p>SLINTECH research has great importance nationally and strategically. If the research data is sold or leaked, rival organizations and foreign nations could use it for competitive advantages or even military purposes. This also poses risks to national security. It has the ability to</p>	<p>(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i></p> <table border="1"> <thead> <tr> <th>Impact Area</th> <th>Value</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation &amp; Customer Confidence</td> <td>8</td> <td>6</td> </tr> <tr> <td>Financial</td> <td>5</td> <td>3.75</td> </tr> <tr> <td>Productivity</td> <td>5</td> <td>3.75</td> </tr> <tr> <td>Safety &amp; Health</td> <td>1</td> <td>1</td> </tr> <tr> <td>Fines &amp; Legal Penalties</td> <td>6</td> <td>4.5</td> </tr> <tr> <td>User Defined Impact Area</td> <td>3</td> <td>2.25</td> </tr> </tbody> </table>			Impact Area	Value	Score	Reputation & Customer Confidence	8	6	Financial	5	3.75	Productivity	5	3.75	Safety & Health	1	1	Fines & Legal Penalties	6	4.5	User Defined Impact Area	3	2.25
Impact Area	Value	Score																							
Reputation & Customer Confidence	8	6																							
Financial	5	3.75																							
Productivity	5	3.75																							
Safety & Health	1	1																							
Fines & Legal Penalties	6	4.5																							
User Defined Impact Area	3	2.25																							

	attract future investment and damage Sri Lanka's scientific reputation.			
		Relative Risk Score	<b>21.25</b>	

### (9) Risk Mitigation

*Based on the total score for this risk, what action will you take?*

Accept

Defer

**Mitigate**

Transfer

**For the risks that you decide to mitigate, perform the following:**

<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>
conference and security awareness workshop	After hiring a new employee, arrange a proper introduction program and keep all workers informed of potential danger. Also, staff must have a clear understanding of data security and be aware of threats and risks to their job roles.
Backup and Recovery	Always maintain secure, regular backups of all sensitive research data and projects frequently.
Restrict the removable media and external storage devices	To reduce insider threats, we could disable USB ports and removable media inputs [12]. Only the authorized person can bring external hard disks and USB drives inside the research labs. Unauthorized copying or transfer, and accidental leaks of sensitive research data. This will minimize internal threats and accidental leaks while maintaining smooth operational efficiency.
	Residual Risks accepted Reputational Impact from attack Human errors Delay detection

Attribute	Value	Justification
Probability	75%	Probability becomes high because study shows that data breaches occur relatively frequently. [11] This will directly affect the ongoing research project, experiment, and sensitive research data. This data exposes that the outside organization or foreign government can cause serious damage to financial reputation and loss of intellectual property.

		Therefore, high impact value is given.
Reputation & Customer Confidence	8	A data breach will cause significant damage to SLINTECH's reputation. If the sensitive research data leaks or is exposed to the outside, it will directly affect the collaborations and partners, and funding agencies. This loss of trust could impact future partnerships and funding opportunities as well. That's why we put high impact value.
Financial	5	According to the study, after the attack, the organization should face significant financial loss. [13] According to the GDPR and ISO/IEC 17025, data protection laws, large organizations should pay costly fines. This will impact ongoing research projects. Therefore, we give high impact value.
Productivity	5	This will directly affect the ongoing research project and cause significant delays due to handling investigations and audits, disrupting the researchers' staff work. These disruption negatively impacts the productivity and research efficiency.
Safety & Health	1	It will have very little impact on the health & safety of a SLINTECH
Fines & Legal Penalties	6	As a result, the Organization should face significant fines and legal penalties according to regional laws like GDPR and ISO/IEC 17025. The study shows that sometimes fines and penalties reach millions of dollars. [14] Therefore, high impact value is given.
User Defined Impact Area	3	SLINTECH conducts some important and critical research. Research delay and financial impact cause significant

		disruption for the researchers and stakeholders.
--	--	--

<b>Allegro - Worksheet 10</b>		<b>INFORMATION ASSET RISK WORKSHEET</b>				
Information Asset Risk	Threat	Information Asset	Research Data			
		Area of Concern	<i>SQL Injection Attack</i>			
		(1) Actor <i>Who would exploit the area of concern or threat?</i>		Outsider Attack		
		(2) Means <i>How would the actor do it? What would they do?</i>		An outsider identifies a weakness in the SLINTECH web application, and an outsider will identify a vulnerable field using SQL injection to gain unauthorized access to the research data. An outsider, after discovering the database and accessing the schema, will modify valid research data in the database.		
		(3) Motive <i>What is the actor's reason for doing it?</i>		Intentional		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>		<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input checked="" type="checkbox"/> Modification <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>		The Outsider modifies the validated research data and corrupts it, which will impact Integrity. An outsider gains access to the database and sensitive research information, which violates confidentiality. Also, the disrupt the database performance will impact the availability. To prevent this, the database backup should be kept under the Organization's control. Ensure the database can only be accessed by SLINTECH authorized members.		
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>		<input type="checkbox"/> High 75%	<input checked="" type="checkbox"/> Medium 50%	<input type="checkbox"/> Low 25%
		(7) Consequences		(8) Severity		

	<i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	<i>How severe are these consequences to the organization or asset owner by impact area?</i>		
		<b>Impact Area</b>	<b>Value</b>	<b>Score</b>
	A successful SQL injection attack can damage several aspects of an SLINTECH reputation. This incident reduces trust among the international collaborators, funding agencies, and researchers.  Can result in significant financial loss for SLINTECH. Also, the organization must invest in security measures to prevent these costly attacks and protect its stability.	Reputation & Customer Confidence	7	3.5
		Financial	6	3
	A successful SQL injection attack can impact several ways in the organization, causing data breaches, system disruption, and temporary shutdown of the database. As a result, the organization should face delays in the experiment, affecting project timelines.  A successful SQL injection attack raises significant safety and health risks, especially in the SLINTECH like research center. By modifying sensitive research data, these attacks can lead to incorrect experimental results.	Productivity	6	3
		Safety & Health	3	1.5
	As a result of a successful SQL injection attack, the Organization may face regulatory fines and legal penalties. This may cause significant financial effects for the organization.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	3	1.5
<b>Relative Risk Score</b>				<b>15</b>

<b>(9) Risk Mitigation</b> <i>Based on the total score for this risk, what action will you take?</i>					
<input type="checkbox"/> Accept <input type="checkbox"/> Defer <input checked="" type="checkbox"/> Mitigate <input type="checkbox"/> Transfer					
<b>For the risks that you decide to mitigate, perform the following:</b>					
<i>On what container would you apply controls?</i>		<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>			
Awareness program	Conduct a training session for IT staff and developers on database security and coding practices. A Regular awareness session will help the staff to make a quick response to a threat.				
Regular software and security patch update	Keep the database system and related software always updated with the latest versions. Ensure the system protects against threats.				
Access and monitoring Logins	Enable access to the logs for databases to track all user activity. Usually, monitoring these logs helps to prevent future threats and quickly respond to potential attacks.				
	Residual Risks accepted  Human errors Incomplete software patching Delay threat detection				

Attribute	Value	Justification
Probability	50%	Probability becomes medium because some studies show that both medium(45%-50%) levels of organization faced one or more successful SQL injection attacks. [15] This indicates the significant level of probability of occurrence; essentially, proper security action is not taken.
Reputation & Customer Confidence	7	A successful SQL injection attack can damage or modify the SLINTECH sensitive research data, and also expose it to the outside competitive organizations and foreign governments. This will lose trust among the international collaborators, funding agencies, and researchers. That's why (7/10) high impact value given.
Financial	4	A successful attack caused significant financial loss for the organization. The study shows this incident can exceed \$19600; some cases lead to multi-million dollar expenses due to system recovery, fines, legal fees, and disruption. [16] The organization must invest in security measures to prevent these costly attacks and protect its stability. Therefore, a high impact value is given.
Productivity	6	SQL injection attacks can impact the organization, causing data breaches, system disruption, and temporary shutdown of the database. As a result, SLINTECH should face several critical problems, including delays in the experiment, which affect project timelines. Therefore, a high impact value is given.(6/10)
Safety & Health	3	Modifying sensitive research data can cause significant safety and health risks. If it leads to incorrect experimental results, it

		will have a direct effect on the ongoing research projects.
Fines & Legal Penalties	5	After a successful SQL injection attack, SLINTECH should face several fines and legal penalties, according to the GDPR and ISO/IEC 17025. [17]Under HIPAA or regional data protection regulations, SLINTECH has to pay millions of dollars in fines. Also, the organization should face lawsuits and audits. This has significant financial damage. That's why we put high impact value(5/10).
User Defined Impact Area	3	The attack will impact financial, collaborators, partnerships, Research projects, and innovations.

### 3. IT232879

#### Central Server

<b>Allegro Worksheet 8</b>			<b>CRITICAL INFORMATION ASSET PROFILE</b>
<b>(1) Critical Asset</b> <i>What is the critical information asset?</i>	<b>(2) Rationale for Selection</b> <i>Why is this information asset important to the organization?</i>	<b>(3) Description</b> <i>What is the agreed-upon description of this information asset?</i>	
SLINTEC Central Server	The SLINTEC Server is necessary part of SLINTEC because it host's research data, intellectual property, lab results, internal applications. It also supports ongoing research collaborations with industry(Brandix,MAS) and drives national innovation goals. Without server both research and administrative functions would face major upheaval	SLINTEC Server is a main asset that supports research, collaboration and administrative tasks. Server manage data, internal applications, analytical services, authentication services used by scientists, researchers, administrators and external collaborators. It also supports day-to-day operations emails and file handling. SLINTEC consists of some advanced mineral elements, electron and molecular recognition machines. The Server also plays pivotal role in storing managing and basic analyzing datasets generated by these instruments.	
<b>(4) Owner(s)</b> <i>Who owns this information asset?</i>			
SLINTEC IT Department			
<b>(5) Security Requirements</b> <i>What are the security requirements for this information asset?</i>			
<input type="checkbox"/> <b>Confidentiality</b>	Only authorized personnel can view this information asset, as follows:	Only the authorized IT administrators and approved scientists should be access to the server. The server stores sensitive data and intellectual property. If unnotarized people view the this data and IP, it could result in lawsuits, reputational damage.	

<input type="checkbox"/> <b>Integrity</b>	Only authorized personnel can modify this information asset, as follows:	Most research and experiments conduct accuracy and trustworthiness of the data and system on the server. Any unauthorized modification could degrade experimental results, invalidate research causing serious financial and reputational loss.
<input type="checkbox"/> <b>Availability</b>	This asset must be available for these personnel to do their jobs, as follows:	The server must be available since scientist and administrative staff rely on it for their day to day tasks. downtime would halt all the operations.
	This asset must be available for <u>24</u> hours, <u>7</u> days/week, <u>52</u> weeks/year.	The server should support 24/7 operations continually with minimum downtime
<input type="checkbox"/> <b>Other</b>	This asset has special regulatory compliance protection requirements, as follows:	Compliance with ISO/IEC 17025:2017 lab accreditation [7], Sri Lanka's Data protection act(no 9 of 2022) [8]

#### (6) Most Important Security Requirement

*What is the most important security requirement for this information asset?*

- |  |                                    |  |                                |
|--|------------------------------------|--|--------------------------------|
| <input type="checkbox"/> Confidentiality | <input type="checkbox"/> Integrity | <input type="checkbox"/> <b>✓ Availability</b> | <input type="checkbox"/> Other |
|--|------------------------------------|--|--------------------------------|

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	SLINTEC Central Server	
	Area of Concern	Environmental and physical hazards (Fire, Power shortages)	
Threat	(1) Actor <i>Who would exploit the area of concern or threat?</i>	Natural Environment , Utility Provider	
	(2) Means <i>How would the actor do it? What would they do?</i>	Electrical shorts, Electrical charge due to poor cable management.  Fire caused by natural disaster (lightning Strike, earthquake damage to wiring), overheating equipment's in server room	

		Flooding from heavy rain fall		
	(3) Motive <i>What is the actor's reason for doing it?</i>	Natural Environment -- No motive Accidental Human error or utility failure		
	(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input checked="" type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption		
	(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Availability- breached if the server is damaged or powered down(downtime) Integrity-Active process may terminate incorrectly due to uncontrolled shutdown or physical damage (data change in unintended ways)		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High 75%	<input type="checkbox"/> Medium 50%	<input checked="" type="checkbox"/> Low 25%
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
	Reputation damage – researchers and industry partners may lose trust to safeguard infrastructure  Financial losses – Hardware replacement, repair cost, loss of funding to research	Impact Area Reputation & Customer Confidence	Value 7	Score 1.75
	Operational Downtime-system unavailability disturbs access to research data, internal applications, collaboration platforms delaying projects and timelines  Research Interruption – corrupted data may invalidate experiments and force to repeat experiments	Impact Area Financial	Value 8	Score 2
		Impact Area Productivity	Value 9	Score 2.25

	Fire and electrical hazard may give risk to employees life.	Safety & Health	8	2	
	Workplace safety and research agreements could result in fines, legal actions.	Fines & Legal Penalties	7	1.75	
		User Defined Impact Area	8	2.	
<b>Relative Risk Score</b>					<b>11.75</b>

#### (9) Risk Mitigation

*Based on the total score for this risk, what action will you take?*

Accept

Defer

Mitigate

Transfer

**For the risks that you decide to mitigate, perform the following:**

On what container would you apply controls?	What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?
Environmental controls	Maintain temperature (18C) and humidity to prevent equipment failures. install antistatic flooring and proper server aisles to prevent hazards. Ensure windowless, ventilated server rooms with 9ft ceilings [18].
Power protection	Implement power surge protection and uninterruptible power supplies (UPS) to safeguard against power outages.  Install fire suppression and smoke detectors.  Maintain a backup power source.
Disaster recovery plans	Conduct periodic security assessments to identify potential disasters.  Conduct Risk assessment and business impact analysis, define recovery strategies, develop disaster recovery procedures, implement preventive and detective controls [19]

Training Exercises	Exercise's for performing mock disaster simulations.  Train staff responsible for disaster prevention and server room management. Train current staff and acquire additional staff if not enough members are available.
Wire and aisle management	Cables should be properly stored to avoid tripping hazards.  Obstacles must be kept out of the server aisle. Keep forbidden items such as flammable materials, food out of server room [20]
	Residual Risks accepted  Unpredictable Natural Disasters  Extended power outages beyond UPS/ Generator Capacity  Supply chain delays of new servers or replacement parts

Attribute	Value	Justification
Probability	25%	Environmental and physical hazards are possible but not constant. Sri Lanka's power fluctuations and high humidity increase the risk of surges and overheating. SLNITC is situated near a river. So, there is a less frequent flooding event.
Reputation & Customer Confidence	7	Damage to server could result in downtime. This could reduce confidence among collaborators, scientists in SLINTEC's ability to safeguard and maintain operations
Financial	8	Financial losses are high. Average cost of server downtime is 12000\$-14000\$. And also, the recovery cost is high. cost for server replacements, potential loss

		of research funding make impact high.
Productivity	9	Server downtime halts the research data access, administrative operations, collaboration among researchers directly reducing their output.
Safety and Health	8	Fire and electrical faults may cause risks to employee (server room) lives but overall exposure is limited.
Fines and Legal Penalties	7	Possible penalties with financial fines, criminal penalties, Operational shutdowns until issues are resolved.
User defined Impact Area	8	SLINTEC conducts some critical research in its facilities. Research delays or corruption force repetition of experiments, causing significant disruption

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	SLINTEC Central Server
		Area of Concern	Exploitation of unpatched vulnerabilities in server
		(1) Actor <i>Who would exploit the area of concern or threat?</i>	Cybercriminals
		(2) Means <i>How would the actor do it? What would they do?</i>	<p>Attackers scan for Vulnerable software/ outdated operating system using tools like Nmap or shodan</p> <p>Deploying exploit code from frameworks like Metasploit or public repositories.</p> <p>To steal Intellectual property, deploy ransomware or disrupt lab operations</p>

	(3) Motive <i>What is the actor's reason for doing it?</i>	Intellectual property theft for competitive advantage, financial gain, Disruption of SLINTEC innovation economy, sabotage ongoing projects.																							
	(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input checked="" type="checkbox"/> <b>Disclosure</b> <input type="checkbox"/> <b>Destruction</b> <input type="checkbox"/> <b>Modification</b> <input type="checkbox"/> <b>Interruption</b>																							
	(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Confidentiality – Exposure of Intellectual property (patent details) Integrity – Data or system configurations altered. Availability – Services disrupted (server crashes) halt server hosted R&D and lab tools.																							
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> <b>High</b> 75%	<input type="checkbox"/> <b>Medium</b> 50%	<input type="checkbox"/> <b>Low</b> 25%																					
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i> <table border="1"> <thead> <tr> <th>Impact Area</th><th>Value</th><th>Score</th></tr> </thead> <tbody> <tr> <td>Reputation &amp; Customer Confidence</td><td>8</td><td>4</td></tr> <tr> <td>Financial</td><td>9</td><td>4</td></tr> <tr> <td>Productivity</td><td>8</td><td>4</td></tr> <tr> <td>Safety &amp; Health</td><td>2</td><td>1</td></tr> <tr> <td>Fines &amp; Legal Penalties</td><td>6</td><td>3</td></tr> <tr> <td>User Defined Impact Area</td><td>8</td><td>4</td></tr> </tbody> </table>			Impact Area	Value	Score	Reputation & Customer Confidence	8	4	Financial	9	4	Productivity	8	4	Safety & Health	2	1	Fines & Legal Penalties	6	3	User Defined Impact Area	8	4
Impact Area	Value	Score																							
Reputation & Customer Confidence	8	4																							
Financial	9	4																							
Productivity	8	4																							
Safety & Health	2	1																							
Fines & Legal Penalties	6	3																							
User Defined Impact Area	8	4																							
	Lawsuits from affected customers.	Relative Risk Score <b>20</b>																							

### (9) Risk Mitigation

*Based on the total score for this risk, what action will you take?*

 Accept

 Defer

 Mitigate

 Transfer

**For the risks that you decide to mitigate, perform the following:**

<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>
SLINTC Server and its software Stack (OS, applications)	<p>Conduct weekly patching cycles – follow a documented process for OS and application patches.</p> <p>Deploy scanning tools (Nessus, Qualys) to identify unpatched software weekly. [21]</p>
Training	Educate IT staff on timely patch deployment and Vulnerability Scanning.
Patch Automation	Deploy OS-native tools and third-party solutions for automated patching, ensuring timely updates. [22]
Service hardening	<p>Remove/disable unnecessary services(telnet,FTP), protocols and default account to minimize attack surface.</p>
	<p>Residual Risks accepted</p> <p>Patch downtime – temporary interruptions during maintenance time.</p> <p>Resource constraints – funding limitations may delay implementations of advanced controls</p> <p>End of life Software -End of OS support or lab tool may remain unpatchable</p>

Attribute	Value	Justification
Probability	50%	SLINTEC's research servers with specialized software are vulnerable to exploits. Existing controls like patching reduce the likelihood from high to moderate. Unpatched servers are among the most exploited attack vectors. (equifax2017) [23] Which justifies probability at medium
Reputation & Customer Confidence	8	Loss of trust in SLINTEC's labs and innovation status due to breach would significantly impact partnerships with industry.
Financial	9	Exploitation could lead to IP theft (\$2.2M Nano fertilizer patents [24]). high recovery cost. Financial losses from disrupted operations are severe for SLINTEC
Productivity	8	Exploits halt critical R&D and lab services, delaying projects impact significantly operational efficiency.
Safety and Health	2	Limited impact until nano material is misused. (nano lab cooling application damaged)
Fines and Legal Penalties	6	Due to breach risks fines and potential legal actions, though less severe than financial or reputational damage.
User defined Impact Area	8	Delay in SLINTEC's contribution to Sri Lanka technology, economy undermining its role and national innovation goals.

## References

- [1] slintec. [Online]. Available: <https://www.slintec.lk/>.
- [2] G. VPS, "Network Disruption: Causes, Impacts, and Solutions," [Online]. Available: <https://blog.greencloudvps.com/network-disruption-causes-impacts-and-solutions.php>. [Accessed 3 october 2025].
- [3] Cloudflare, "What is a distributed denial-of-service (DDoS) attack?," [Online]. Available: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>. [Accessed 3 october 2025].
- [4] Cloudflare, "What is a distributed denial-of-service (DDoS) attack?," [Online]. Available: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>. [Accessed 3 october 2025].
- [5] Eclypsium, "Unpacking NIST Hardware and Firmware Security Failure Scenarios," [Online]. Available: <https://eclypsium.com/blog/nist-hardware-firmware-security-failure-scenarios/>. [Accessed 3 october 2025].
- [6] D. Piper, "Data Protection Laws of the World," [Online]. Available: <https://www.dlapiperdataprotection.com/>. [Accessed 2 october 2025].
- [7] iso, "iso," [Online]. Available: <https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html>.
- [8] d. p. authority. [Online]. Available: <https://www.dpa.gov.lk/>.
- [9] M. Buckbee, "varonis," 25 feb 2022. [Online]. Available: <https://www.varonis.com/blog/company-reputation-after-a-data-breach>. [Accessed 3 feb 2025].
- [10] H. D. W. Ping Wang, "ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES," *International Association for Computer Information Systems*, vol. 20, no. 2, p. 162, 2019.
- [11] E. Bonnie, "secureframe," 4 sep 2025. [Online]. Available: <https://secureframe.com/blog/data-breach-statistics>. [Accessed 3 oct 2025].
- [12] B. Danial, "trentonsystems," 19 feb 2021. [Online]. Available: <https://www.trentonsystems.com/en-us/resource-hub/blog/why-computer-manufacturers-disable-usb-ports>. [Accessed 3 oct 2025].

- [13] asimily, "asimily," [Online]. Available: <https://asimily.com/blog/4-cyberattacks-universities-and-colleges/>. [Accessed 3 Oct 2025].
- [14] vismaya, "vismaya," [Online]. Available: <https://vismayacorp.com/data-breach-fines-2025/>. [Accessed 3 Oct 2025].
- [15] S. Citakovic, "securityescape," 23 may 2023. [Online]. Available: <https://securityescape.com/sql-injection-attacks-statistics/>. [Accessed 2 oct 2025].
- [16] Attack Prevention, "Protecting Financial Applications from SQL Injection Attacks," *Protecting Financial Applications from SQL Injection Attacks*, 21 jan 2025.
- [17] E. Johnson, "ihasco," [Online]. Available: <https://www.ihasco.co.uk/blog/data-protection-fines-recent-years>. [Accessed 3 Oct 2025].
- [18] zenarmor, "zenarmor," [Online]. Available: <https://www.zenarmor.com/docs/network-security-tutorials/what-is-server-security>.
- [19] j. fellows, "liquidweb," [Online]. Available: <https://www.liquidweb.com/blog/server-disaster-recovery/>.
- [20] v. tech, "virginia tech," [Online]. Available: <https://security.vt.edu/procedures/server-physical-protection/>.
- [21] NIST. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf>.
- [22] kanooelite. [Online]. Available: <https://www.kanooelite.com/server-operating-system-security/>.
- [23] eqaifix, "spamtitan," [Online]. Available: <https://www.spamtitan.com/blog/poor-patch-management-policies-to-blame-for-equifax-data-breach/>.
- [24] wikipedia. [Online]. Available: [https://en.wikipedia.org/wiki/Sri\\_Lanka\\_Institute\\_of\\_Nanotechnology](https://en.wikipedia.org/wiki/Sri_Lanka_Institute_of_Nanotechnology).