ID	Asset / Process	Threat	Vulnerability
R01	Student records	Data breach / Theft	No encryption on sensitive data
R02	PC / Laptop	System corruption / Data loss	Untracked removable media use
R03	Teaching website platform	Malware injection	No patch management process
R04	Personal email account	Phishing attack	Lack of two-factor authentication
R05	Cloud storage service	Unauthorized access	Weak permissions and access control
R06	Instructor / Staff	Human error	No awareness of security policy
R07	Printed documents	Data leak	Documents left on desk or printer
R08	Lesson scheduling software	System downtime	No redundancy / Single point of failure
R09	WiFi	Eavesdropping	Default network credentials
R10	Network router	Physical tampering	Router left exposed
R11	Student communication	Data leak by email	No secure messaging policy
R12	Office workspace / Electrical supply	Power failure or surge	No surge protection or UPS
R13	Payment process	Fraudulent transaction	Weak verification process
R14	Old laptop or external drive	Improper disposal or reuse	Not wiped before disposal

Risk Description	Likelihood (1-5)	Impact (1-5)	Inherent Risk (LxI)
Loss or theft of laptop could expose student data	4	5	20
Untracked removable media use	4	4	16
Outdated software could be exploited by attackers	3	4	12
Phishing email could compromise credentials	4	3	12
Improper access control could lead to data leakage	3	4	12
Lack of cybersecurity awareness training	4	3	12
Sensitive information may be seen or taken	3	3	9
Disruptions causing missed lessons and client impact	3	3	9
Unsecured network allows interception of business data	3	3	9
Unauthorized reset or changes to configurations	3	3	9
Sharing of private data with unauthorized parties	3	3	9
Power outage may disrupt teaching or corrupt data	3	3	9
Fraudulent transaction or payment misdirection	2	4	8
Residual data could be recovered	2	4	8

Control (Annex A ref)	Control Domain	Residual Likelihood	Residual Impact	Residual Risk (LxI)	Risk Owner
A.8.11 – Data Encryption	Technological	2	3	6	IT Manager
A.8.10 – Use of Removable Media	Technological	2	3	6	IT Manager
A.5.23 – Change Management	Organizational	2	3	6	Web Admin
A.5.17 – Authentication Information	Organizational	2	3	6	All Staff
A.8.25 – Cloud Services Security	Technological	2	3	6	CISO
A.6.3 – Information Security Awareness	People	2	2	4	All Staff
A.7.3 – Securing Offices, Rooms, and Facilities	Physical	2	2	4	Staff
A.5.28 – Capacity Management	Organizational	2	2	4	Admin
A.8.9 – Configuration Management	Technological	2	2	4	IT Manager
A.7.6 – Equipment Siting and Protection	Physical	2	2	4	IT Manager
A.5.10 – Acceptable Use of Information	Organizational	2	2	4	All Staff
A.7.9 – Supporting Utilities	Physical	2	2	4	Facility / IT
A.8.20 – Supplier Relationships	Organizational	1	2	2	Finance / Admin
A.7.12 – Secure Disposal or Reuse of Equipment	Physical	1	2	2	IT Manager

Status / Notes
Implement encryption and backup procedures
Block unauthorized USB use and scan media
Update website monthly and test patches
Enable MFA and phishing training
Quarterly access reviews for cloud storage
Conduct quarterly awareness training
Enforce clear desk policy and secure storage
Setup failover or backup scheduler
Change Wi-Fi password regularly and enable WPA3
Lock network equipment cabinet
Use secure file-sharing platform for student data
Install surge protector and UPS for key equipment
Verify payments using dual approval process
Physically destroy drives before disposal