Certainly! I'll provide you with five Information Asset Risk Worksheets for Horizon University in Malabe, Sri Lanka. Please note that since I don't have access to internal technical information, the components will be hypothetical. Here are the worksheets:

---

### Information Asset Risk Worksheet 1:

#### Asset: Student Database

- \*\*Description:\*\* Contains personal information (names, addresses, contact details) of all enrolled students.

- \*\*Value:\*\* High

- \*\*Vulnerabilities:\*\*

- Lack of encryption in transit and at rest.

- Insufficient access controls for database administrators.

- \*\*Threats:\*\*

- Unauthorized access by internal staff.

- External cyberattacks targeting student data.

- \*\*Impact:\*\*

- Financial loss due to legal fines for data breaches.

- Reputational damage and loss of trust.

---

### Information Asset Risk Worksheet 2:

#### Asset: Research Databases

- \*\*Description:\*\* Contains sensitive research data, intellectual property, and grant-related information.

- \*\*Value:\*\* Critical

- \*\*Vulnerabilities:\*\*

- Inadequate data encryption and access controls.

- Lack of regular security audits and patching.

- \*\*Threats:\*\*

- Insider threats from disgruntled researchers.

- Advanced persistent threats targeting research findings.

- \*\*Impact:\*\*

- Loss of competitive advantage if research data is compromised.

- Legal repercussions for mishandling grant-related information.

---

### Information Asset Risk Worksheet 3:

#### Asset: Financial System

- \*\*Description:\*\* Contains sensitive financial data, including payroll information, budget allocations, and transaction records.

- \*\*Value:\*\* Critical

- \*\*Vulnerabilities:\*\*

- Weak authentication and authorization mechanisms.

- Insufficient auditing of financial transactions.

- \*\*Threats:\*\*

- Fraudulent activities from internal staff.

- External cyberattacks aiming to manipulate financial records.

- \*\*Impact:\*\*

- Financial losses due to embezzlement or fraudulent transactions.

- Legal penalties for non-compliance with financial regulations.

---

### Information Asset Risk Worksheet 4:

#### Asset: Learning Management System (LMS)

- \*\*Description:\*\* Houses course materials, assessments, and student performance records.

- \*\*Value:\*\* High

- \*\*Vulnerabilities:\*\*

- Weak password policies and lack of multi-factor authentication.

- Insufficient monitoring of user activities.

- \*\*Threats:\*\*

- Unauthorized access leading to grade tampering.

- Distributed denial-of-service attacks on the LMS platform.

- \*\*Impact:\*\*

- Academic integrity compromised due to grade manipulation.

- Disruption of education services during attacks.

---

### Information Asset Risk Worksheet 5:

#### Asset: Employee Personal Information

- \*\*Description:\*\* Contains employee records, including HR files, personal contact details, and performance evaluations.

- \*\*Value:\*\* High

- \*\*Vulnerabilities:\*\*

- Inadequate access controls for HR personnel.

- Lack of employee training on data protection.

- \*\*Threats:\*\*

- Unauthorized access by employees seeking sensitive information.

- Phishing attacks targeting HR staff for login credentials.

- \*\*Impact:\*\*

- Breach of privacy laws leading to legal repercussions.

- Decreased employee morale and trust.

---

Please note that these worksheets are hypothetical and based on general information security best practices. Horizon University in Malabe should conduct a thorough risk assessment with input from their IT and security teams to create specific and accurate risk assessments.

Certainly, let's create five Information Asset Risk Worksheets for Horizon University in Malabe, Sri Lanka. Please note that the information provided here is fictional, as I don't have access to real data. These worksheets will help identify and assess potential risks to the university's information assets.

\*\*Information Asset Risk Worksheet 1: Student Records Database\*\*

1. \*\*Asset Description:\*\* Student Records Database

2. \*\*Asset Owner:\*\* Dean of Academic Affairs

3. \*\*Asset Location:\*\* University Data Center

4. \*\*Asset Value:\*\* High

5. \*\*Threats:\*\*

a. Unauthorized access to student records

b. Data breaches due to weak access controls

c. Data loss due to hardware failure

d. Insider threats (e.g., faculty or staff mishandling data)

6. \*\*Vulnerabilities:\*\*

a. Outdated security protocols

b. Insufficient encryption

c. Lack of regular security audits

d. Inadequate staff training

7. \*\*Impact:\*\* Reputation damage, legal consequences, financial loss

8. \*\*Likelihood:\*\* Moderate

9. \*\*Risk Level:\*\* High

\*\*Information Asset Risk Worksheet 2: Financial Systems\*\*

1. \*\*Asset Description:\*\* Financial Systems

2. \*\*Asset Owner:\*\* Chief Financial Officer (CFO)

3. \*\*Asset Location:\*\* Finance Department

4. \*\*Asset Value:\*\* High

5. \*\*Threats:\*\*

a. Unauthorized access to financial data

b. Fraudulent activities

c. Malware or ransomware attacks

d. Inadequate disaster recovery planning

6. \*\*Vulnerabilities:\*\*

a. Weak authentication mechanisms

b. Lack of real-time monitoring

c. Inadequate backup procedures

d. Insufficient user training

7. \*\*Impact:\*\* Financial loss, regulatory fines, operational disruption

8. \*\*Likelihood:\*\* Low to Moderate

9. \*\*Risk Level:\*\* High

\*\*Information Asset Risk Worksheet 3: Research Data Repository\*\*

1. \*\*Asset Description:\*\* Research Data Repository

2. \*\*Asset Owner:\*\* Director of Research

3. \*\*Asset Location:\*\* University Library

4. \*\*Asset Value:\*\* Moderate

5. \*\*Threats:\*\*

a. Unauthorized access to research data

b. Data corruption or loss

c. Data theft by competitors

d. Lack of data backup

6. \*\*Vulnerabilities:\*\*

a. Inadequate access controls

b. Insufficient data encryption

c. Lack of data redundancy

d. Limited staff awareness

7. \*\*Impact:\*\* Loss of research findings, reputation damage

8. \*\*Likelihood:\*\* Moderate

9. \*\*Risk Level:\*\* Moderate

\*\*Information Asset Risk Worksheet 4: Student Portal\*\*

1. \*\*Asset Description:\*\* Student Portal

2. \*\*Asset Owner:\*\* Director of IT

3. \*\*Asset Location:\*\* University Website

4. \*\*Asset Value:\*\* Moderate

5. \*\*Threats:\*\*

a. Distributed denial-of-service (DDoS) attacks

b. Data breaches leading to student data exposure

c. Malware infections through the portal

d. Phishing attacks targeting students

6. \*\*Vulnerabilities:\*\*

a. Inadequate web security measures

b. Lack of intrusion detection systems

c. Unpatched software

d. Limited user education on online safety

7. \*\*Impact:\*\* Disruption of services, loss of student trust

8. \*\*Likelihood:\*\* Low to Moderate

9. \*\*Risk Level:\*\* Moderate

\*\*Information Asset Risk Worksheet 5: Human Resources Database\*\*

1. \*\*Asset Description:\*\* Human Resources Database

2. \*\*Asset Owner:\*\* Director of Human Resources

3. \*\*Asset Location:\*\* HR Department

4. \*\*Asset Value:\*\* High

5. \*\*Threats:\*\*

a. Unauthorized access to employee records

b. Data breaches exposing sensitive HR information

c. Insider threats (e.g., disgruntled employees)

d. Data loss due to inadequate backup

6. \*\*Vulnerabilities:\*\*

a. Weak access controls

b. Lack of employee training on security

c. Insufficient data encryption

d. Inadequate employee background checks

7. \*\*Impact:\*\* Legal consequences, reputational damage, operational disruption

8. \*\*Likelihood:\*\* Moderate

9. \*\*Risk Level:\*\* High

These Information Asset Risk Worksheets can be used by Horizon University in Malabe to assess and manage the risks associated with their critical information assets. It's important for the university to regularly review and update these assessments to stay proactive in mitigating potential threats.