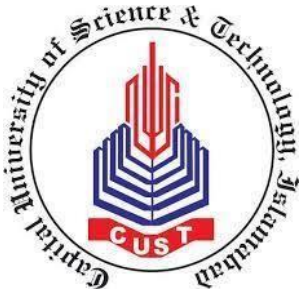



# Capital University of Science & Technology

# Islamabad, Pakistan

## Major Assignment – Scenario Based Project

---

## CS3713: Introduction to Information Security and Forensics

## (S3)

**Group Members:**

**Hajra Hassan Toor**

**BCS203258**

**Rafiya Tariq**

**BCS203031**

**January 17, 2023**

---

# International Islamic University, Islamabad


الجامعة الاسلامية العالمية

International Islamic University, Islamabad

# Introduction:

The **International Islamic University, Islamabad,** or IIUI, **(Arabic: الجامعة الإسلامية العالمية إسلام آباد, Urdu: بین الاقوامی اسلامی یونیورسٹی اسلام آباد)** is a public research university located in Islamabad, Pakistan. It was established in 1980 and restructured in 1985, and remains a valuable source for Higher Education in Pakistan. The university is regularly listed among the most recognized universities and prestigious degree awarding institutions of Pakistan by the Higher Education Commission of Pakistan. The university ranks joint second in the 2022 top university rankings of Times Higher Education World University Rankings in Pakistan. It also constantly ranks among the best universities in the country for the general category by Higher Education Commission of Pakistan.

The university is a center of Islam, theology and the Islamic studies in a contemporary context . The university was founded in 1980 with funding from inside Pakistan and foreign donations from Saudi Arabia. The university provides education and training in Islamic law for the professions of judicial officers, public prosecutors, teachers of madrassas, preachers of Friday sermons and imams.

It attracts students from the country and from Central and Southeast Asia. In 2012, the university was ranked fourth in the category of general universities by the Higher Education Commission (Pakistan). In February 2014, she awarded an honorary doctorate in politics and international relations to King Abdullah of Saudi Arabia. It offers undergraduate and graduate programs in law, science, engineering and technology, humanities, arts, religious studies, social and natural sciences.

# *Introduction to Security Policies of International Islamic University of Pakistan:*


Users of International Islamic University network and computer resources have a responsibility to properly/fairly use and protect those information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information technologies.

## *Integrity of Information Resources:*

Computer users must respect the integrity of computer-based information resources.

- **Modification or Removal of Equipment** Computer users must not attempt to modify or remove computer equipment, software, or peripherals as these are the property of the University.
- **Encroaching on Others' Access and Use Computer** Users must not encroach on other's access and use of the University's computers, networks, or other information resources, including digital information. This includes but is not limited to attempting to access or modify personal, individual or any other University information or other resources for which the user is not authorized; sending chain-letters, unsolicited bulk electronic mail either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the users; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer, network or other information resources; or otherwise damaging or vandalizing University computing facilities, equipment, software, computer files or other information resources.
- **Unauthorized or Destructive Programs** Computer users must not intentionally develop or use programs which disrupt other computer or network users or which access private or restricted information or portions of a System and / or damage software or hardware components of a system. Computer users must ensure that they don't use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in legal action for damages or other punitive action by any injured party, including the University.

## ***Privacy:***

Users connected to the network must not try to violate the privacy of the other users in the network. System administrators will report suspected unlawful or improper activities to the proper authorities.

i. Political Use: University information resources will not be used for partisan political/religious/ labour-welfare activities.
ii. Personal Use: University information resources should not be used for personal activities not related to appropriate University functions.
iii. Commercial Use: University information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the University or with the written approval of a university authorities having the authority to give such approval. Any such commercial use should be related to university activities.

## ***Unauthorized Access:***

Computer users must refrain from seeking to gain unauthorized access to information resources/services or enabling unauthorized access.

- **Reporting Problems** Any defects discovered in the system as well as in the network must be reported to the appropriate system administrator deputed in local IT Support

Office, so that steps can be taken to investigate and resolve the problem. The problem can be reported on the telephone, via official email or in writing, at the respective blocks IT Support Offices.

- **Password Protection** A computer user who has been authorized to use a password may be subject to disciplinary action if the user discloses the password or otherwise makes the account available to others without permission of the system administrator. For protecting sensitive data, it is always advisable to use strong passwords & avoid common or easily guessable names.

# Analysis of all Security Policies:

## 1. *Network Security:*

- **Security of IT Equipment at Hostels:**
  The security of the IT equipment installed at Hostels, is the responsibility of the Hostel Administration and the Security Guard on duty. The IT Center will only provide technical support according to the complaints, the keys of the cabinets will be kept by the hostel administration and whenever required any maintenance job, the IT Center will take it and return back after completion of the job. Proper log of usage of these keys will be maintained in a register placed in Hostel's Admin Offices.
- **Internet Services in the University**: The Internet and related services in the University will be provided centrally from Network Operation Center (NOC) to all the offices/academic blocks of the University. The following will be must to cope with security demands of the Government Agencies:
  - All computer systems in the University premises must be part of the centralized Network Domain.
  - A unique username/password will be issued to each student, and employee.
  - The Internet service will be only accessible from the computers joined on Domain, and without Domain credentials, the Internet services will not be provided.

## 2. *Communication Security:*

- **The IT Staff:**
  The IT manpower working in different Faculties, Administration, Institutes will work under the administrative control of IT Center. The IT Center periodically has to rotate the IT support staff from one Institute/Faculty/Office to another according to their performance and to get knowledge of the services at different departments. The IT Center Staff matters like, leaves, ACRs, Promotions will be written by the IT Center.

## 3. *Application Security Policy:*

After researching this website, we saw their application security policies. Then we check that the connection is secure or not and after that we saw the details of their certificates.

Certificate Viewer: *.iiu.edu.pk

**General** Details

### Issued To

| | |
|---|---|
| Common Name (CN) | *.iiu.edu.pk |
| Organization (O) | <Not Part Of Certificate> |
| Organizational Unit (OU) | <Not Part Of Certificate> |

### Issued By

| | |
|---|---|
| Common Name (CN) | E1 |
| Organization (O) | Let's Encrypt |
| Organizational Unit (OU) | <Not Part Of Certificate> |

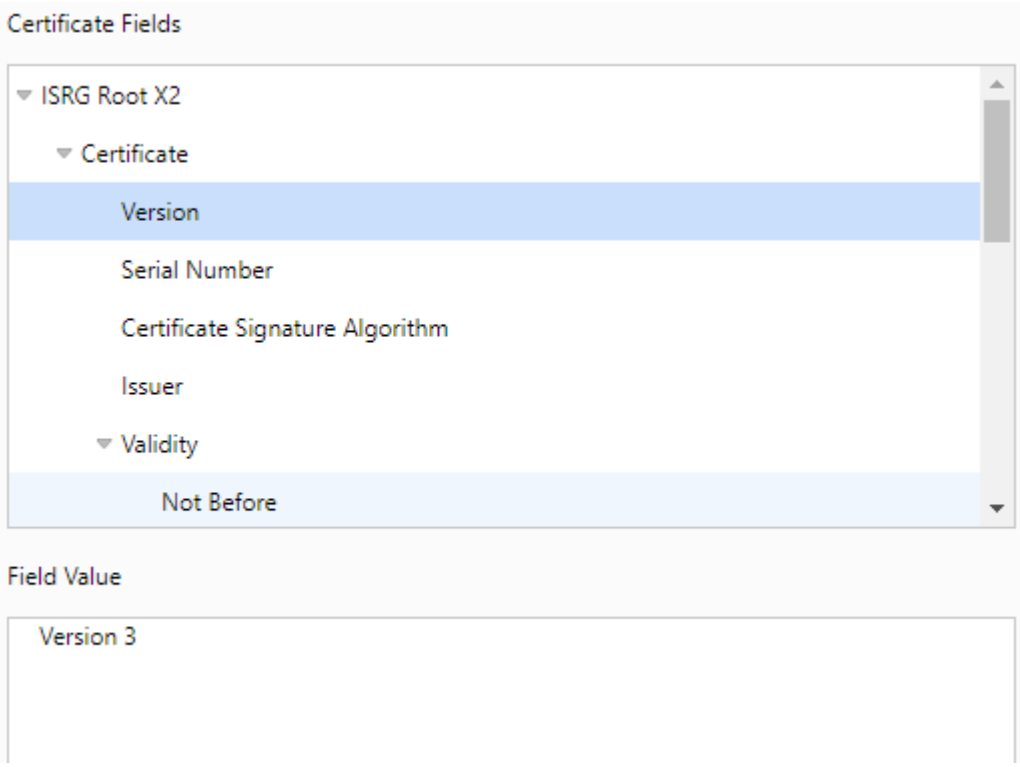
### Validity Period

| | |
|---|---|
| Issued On | Saturday, November 26, 2022 at 7:10:35 AM |
| Expires On | Friday, February 24, 2023 at 7:10:34 AM |

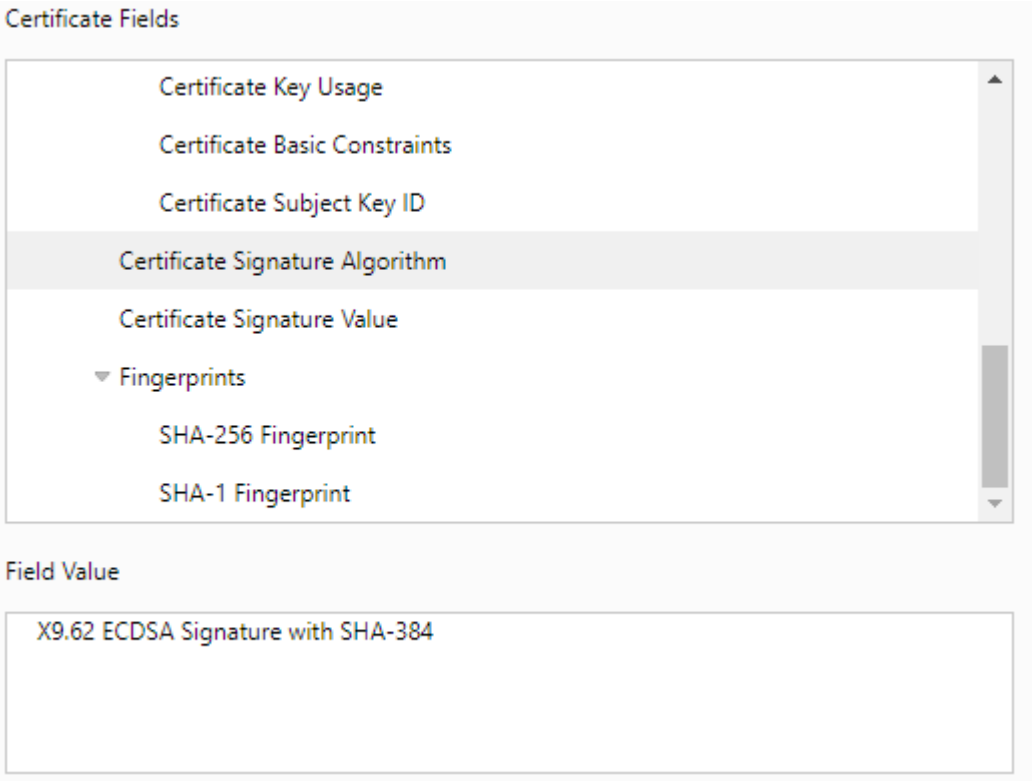
### Fingerprints

| | |
|---|---|
| SHA-256 Fingerprint | AA 01 06 12 B8 B7 7A 09 78 8A 69 88 C7 03 C8 7F 6C F3 1E FD 45 08 32 B6 40 15 5E 89 47 ED F0 18 |
| SHA-1 Fingerprint | ED 28 9A 37 DD A5 40 91 81 DE 2C 18 2C 6E BE 90 FA 6C DA 48 |

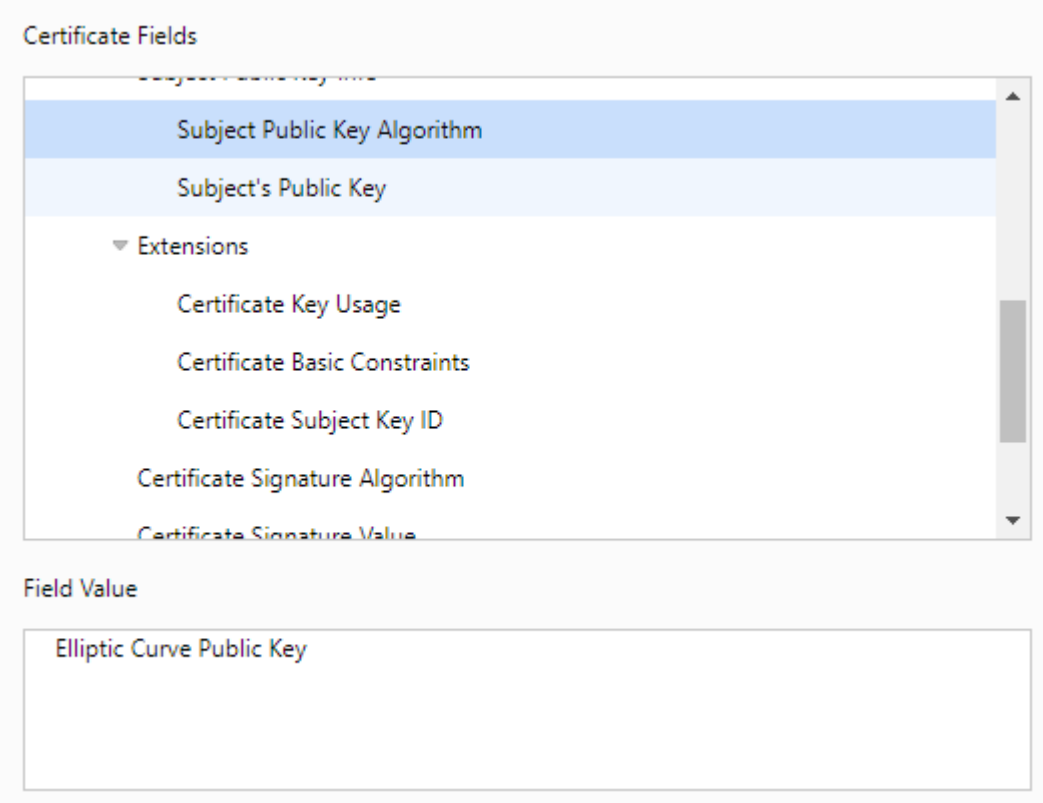
***Version:***




***Signature algorithm:***



***Public Key:***




## 4. ***Risk Assessment Policy:***

Managing risks are crucial in all fields. Information technology risks pose more threats to organizations in three categories:
1. technical and operational risk
2. data and information security risk
3. organization, project and human risk.

Modern organizations must therefore face new and growing IT risk threats in more sophisticated ways. This task is difficult if it is not properly given due care by senior management and is not conscientiously implemented with the duty of care of the responsible teams. The main objective of the paper is to develop an information technology risk management framework for the International Islamic University of Malaysia (IIUM) based on a series of consulting group discussions, risk management formulation, business process identification, risk weight quantification and classification of major risk factors in the university environment. The proposed risk management method was applied to the IIUM case. This study uses an action research approach with the active involvement of researchers and stakeholders to identify, analyze and respond to risks. The analysis is based on both empirical research and a real case study. The study found that senior management recognizes the important pervasive role of information technology in organizations and that the consequent threats arising from and created by the use of IT hardware and software can be detrimental to organizational effectiveness and efficiency. The risk could cause financial loss, loss of privacy, security and data. As a result, IIUM engaged its ICT

strategic business unit to design and draft a new IT risk management framework based on current issues and settings. However, this framework can be applied to other Malaysian public and private universities. Moreover, with a few minor modifications, it is also suitable for replication in non-academic institutions.

## Discussion on Findings:

The findings of the policies implemented by the ***International Islamic University of Pakistan*** show that the department has been successful in protecting the university from various types of threats. The department's comprehensive, multi-security approach, which includes policy development and implementation in areas such as network security, communications, application security, and risk analysis, is effective in addressing a variety of security challenges. For example, a network security policy that emphasizes strong access control, regular monitoring and evaluation, incident response.

Similarly, a communications security policy has been put in place that emphasizes the use of secure and ethical communications methods, as well as regular monitoring and evaluation, incident response, business continuity planning and continuous improvement to protect sensitive information and communications from unauthorized access, disclosure or destruction.

Similarly, an application security policy focused on secure development practices, regular monitoring and analysis, incident response and business continuity planning, and continuous improvement helped protect applications and data from access. Unauthorized access, disclosure or infringement. A risk analysis process that emphasizes the use of risk management methods, monitoring and evaluating risks and mitigation measures, engaging in ongoing activities, identifying and identifying risks that may affect national security and critical infrastructure, and bringing resources to efforts to effectively address the most pressing threats facing the country.

In conclusion, the findings and policies implemented by the **International Islamic University of Pakistan** show that the department has been successful in protecting the university from various threats. The department's comprehensive and comprehensive approach to security has proven effective in addressing a variety of security challenges, including network security, communications security, application security and risk analysis. Regular monitoring and evaluation of this policy, including the use of threat intelligence, vulnerability assessments, and other tools, helps the department adapt to the ever-changing threat landscape.

## Conclusion and Recommendation:

The International Islamic University of Pakistan plays a key role in protecting the country and its citizens from various threats. Departmental and regional policies such as network security, communications security, application security, and risk assessment are effective in addressing various security issues. Policy findings show that the department has been successful in protecting the nation's IT infrastructure and networks, sensitive information and communications, applications and data, and critical assets from unsupported access, disclosure, or breach.

However, it is important to recognize that the threat landscape is constantly changing and it is important for the Department to review and update its policy to adapt to new emerging threats. In addition, it is important to maintain strong relationships with other federal, state, local, and tribal agencies, as well as private companies, to share information and coordinate efforts to protect the nation from various threats.

In light of the above, the findings and policies implemented by the **International Islamic University of Pakistan** show that the department has been successful in protecting the university from various threats. The department's comprehensive and comprehensive approach to security has proven effective in addressing a variety of security challenges, including network security, communications security, application security and risk analysis. Regular monitoring and evaluation of this policy, including the use of threat intelligence, vulnerability assessments, and other tools, helps the department adapt to the ever-changing threat landscape.

## References:

Here are some references:


- https://www.iiu.edu.pk/?page_id=11941
- https://www.iiu.edu.pk/?page_id=22903
- https://www.iiu.edu.pk/wp-content/uploads/downloads/notifications/2015/july/I.T.Usage-Policy.pdf
- https://www.google.com/search?q=what+is+the+risk+assessment+of+international+islamic+university&rlz=1C1UEAD_enPK1030PK1030&sxsrf=AJOqlzWEIXZp3BM6_ymhGT0htRaVBBlxJA%3A1674017667627&ei=g3vHY8TsJdqJkdUPtdWioAs&oq=what+is+the+risk+assessment+of+international+is&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAxgBMgUIIRCgATIFCCEQoAEyBQghEKABMgUIIRCgATIICCEQFhAeEB0yCAghEBYQHhAdMggIIRAWEB4QHTIICCEQFhAeEB06BAgAEEc6BAgjECc6BwgjEOoCECc6DQgAEI8BEOoCELQCGAE6BQgAEJECOgsIABCABBCxAxCDATIECAAQQzoKCAAQsQMQgwEQQzoKCAAQgAQQhwIQFDoNCAAQgAQQsQMQgwEQCjoMCAAQgAQQhwIQChAUOgQIABADOggIABCxAxCDATIICAAQgAQQsQM6BQgAEIAEOgUIABCxAzoGCAAQFhAeOggIABAWEB4QCjoICAAQFhAeEA86BQgAEIYDOgcIIRCgARAKOgQIIRAVOgoIIRAWEB4QDxAdSgQIQRgASgQIRhgBUJMbWOgQAmDdqwJoBHACeASAAfwCiAGYgAGSAQcyLTQ4LjExmAEAoAEBsAEUyAEIwAEB2gEGCAEQARgK&sclient=gws-wiz-serp