Read this first

This file is a **sample synopsis (project proposal)** made by the ignouproject.com editorial desk as study reference for IGNOU MSCIS (and PGDIS) learners doing **MSEP 28 (Project-I)** or **MSEP 38 (Project-II)**. It is not an IGNOU document, it is not an approved proposal, and it must not be submitted as your own work.

It was prepared in November 2026 with AI assistance from the MSEP-028/MSEP-038 Project Guidelines of the School of Vocational Education and Training (SOVET), IGNOU (the PDF file's own properties give a creation date of March 2022), and the IGNOU Common Prospectus, July 2026. Each rule quoted here was checked against those documents, and the file is published under BK Sahni's editorial responsibility.

What the guidelines ask for in a proposal (section V, page 7): eight parts, in this order: Title of the Project; Introduction and Objectives of the Project; Project Category; Research Methodology; Scope of the solution; Analysis; Future scope and further enhancement of the project; Bibliography and Literature survey. This sample follows the same order.

Length: page 5 of the guidelines asks for a proposal of 12 to 15 pages, while section V on page 7 says 15 to 20 pages. A proposal of about 15 pages satisfies both lines. This sample is shorter on purpose, because it shows the shape of each part and leaves the content to you.

Send the proposal with the filled and signed proforma (page 5 of the guidelines) to your own Study Centre, in the slot of 1 January to 15 March or 1 July to 15 September.

Words in square brackets, such as [City] or [number], mark facts only you can supply from your own work. Fill them from your own setting and your own records. Approval of a proposal is decided by IGNOU's Project Proposal Evaluator; your Study Centre is the place to ask about your case.

ignouproject.com is an independent service and is not affiliated with or endorsed by IGNOU.

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION

SAMPLE PROJECT PROPOSAL

Course Code: MSEP-028 (Project-I), MSCIS / PGDIS

Enrolment No.: [your enrolment number] | Study Centre: [code] | Regional Centre: [name and RC code]

(i) Title of the Project

Backup and Restore Readiness of a Small-Office File Server against a Simulated Ransomware Event: A Lab Study Modelled on [Organisation], [City]

Why this wording: the title names the system (a small-office file server), the threat (a simulated ransomware event), the method (a lab study) and the setting. Keep this title word for word on the proforma, the cover page and every page header, because section VI asks that the title stay the same as the approved proposal.

(ii) Introduction and Objectives of the Project

Many small offices keep their shared files on one server or one network folder. When ransomware encrypts those files, the office can work again only if a usable backup exists and can be restored in time. NIST Special Publication 800-34 Rev. 1 treats this as contingency planning and asks an organisation to fix a recovery time objective (how long a system may stay down) and a recovery point objective (how much recent data the organisation can afford to lose) (Swanson et al., 2010). NIST Special Publication 800-184 adds that recovery plans should be tested and improved, not only written (Bartock et al., 2016).

In India, the CERT-In Directions of 28 April 2022, issued under sub-section (6) of section 70B of the Information Technology Act, 2000, require covered entities to report specified cyber incidents to CERT-In within six hours of noticing them (CERT-In, 2022). A small office therefore needs to know quickly what was hit and what can be restored. [Two or three sentences on why [Organisation] or offices like it in [City] were chosen, in your own words.]

Objectives

- To document the backup arrangement of a small-office file server rebuilt in an isolated lab and modelled on the practice at [Organisation].

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION

- To measure the time taken to restore a set of test files from each backup copy (same-disk copy, second disk, disconnected disk) after a simulated encryption event.
- To compare the measured restore time and data loss with the recovery targets written in a short recovery plan for the office.
- To identify gaps between the written recovery plan and the restore steps observed in the lab.

The objectives use neutral verbs (to document, to measure, to compare, to identify) and assume no result in advance.

(iii) Project Category

Lab-based study: implementation, testing and evaluation in an isolated virtual environment. The MSEP-028/038 guidelines do not print a list of categories, so state your category plainly in one line, and say whether the study is a real-life project in an organisation or a problem you have formulated yourself (both are allowed by section IV).

Courses this study draws on: MSEI-026 (BCP, DR Planning and Audit) and MSEI-027 (Digital Forensics), both in Semester II of MSCIS and PGDIS.

(iv) Research Methodology

Element	Plan (fill the brackets from your own lab)
Design	Experimental lab test with repeated trials: [3] runs for each backup copy.
Environment	Two virtual machines on a host-only network with no internet connection: one file server ([operating system and version]) and one client. Only systems the student owns are used.
Test data	[number] dummy files ([total size] GB) generated for the study. No personal or office data.
Event simulation	A harmless script, written and run only inside the lab server, renames and overwrites copies of the dummy files to mimic the effect of encryption. No real malware sample is downloaded or used.
Backup copies	[backup tool and version] writing to (a) a folder on the same disk, (b) a second virtual disk, (c) a disk detached after each backup.
Measures	Restore time in minutes; age of the last good backup (recovery point); share of files restored intact, checked by comparing SHA-256 hashes taken before and after.
Recovery targets	Written in advance in a one-page recovery plan: restore within [hours], lose no more than [hours] of work.

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION

Element	Plan (fill the brackets from your own lab)
Evidence	The student's own logs, command output, hash lists and screenshots, each dated and numbered.
Permission	Our advice, not an IGNOU rule: if the setup is modelled on [Organisation], keep a signed letter from [designation] allowing you to describe its backup practice. No test touches the organisation's live systems.
Analysis tools	Tables of restore time and recovery point for each copy and run; mean and range; a plan-versus-observation gap table.

Accessing a computer system without the permission of its owner attracts penalty and compensation under section 43 of the Information Technology Act, 2000. That is why every test in this plan stays inside a lab the student owns.

(v) Scope of the solution

Included	Excluded
One file server and one client in an isolated lab; three backup copies; restore tests; a one-page recovery plan and its gap table.	Live office systems; real ransomware samples; network intrusion testing; cloud backup services; any personal data.

Limitations to state honestly: a lab rebuild is simpler than a real office; restore times depend on the student's hardware ([processor, memory, disk type]); [three] runs per copy show a pattern, not a general law.

(vi) Analysis

The proposal explains how the evidence will be analysed. It reports no results, because the work has not been done yet.

Objective	Planned analysis	Table or figure in the report
1	Description of the backup arrangement against the recovery plan	Table: backup copies, schedule, location
2	Restore time and files intact for each copy and run	Table: copy x run, minutes, files intact
3	Measured values compared with the written targets	Table: target, observed, met or not met
4	Plan steps compared with observed steps	Gap table: step, written, observed, gap

(vii) Future scope and further enhancement of the project

The same test can be repeated with a cloud backup service or with backups that cannot be changed once written, and over several months to see whether restore time drifts. A related idea may suit MSEP-038 (Project-II) in Semester IV, where the guidelines list cloud server

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION

implementation and security among the areas; the guidelines do not say whether Project-II may extend Project-I, so ask your Study Centre before you plan on it.

(viii) Bibliography and Literature survey

Literature survey (outline). Swanson et al. (2010) set out the contingency planning process and define recovery time and recovery point objectives. Bartock et al. (2016) focus on recovering from cyber events and on testing recovery plans with exercises and metrics. The CERT-In Directions (2022) set the Indian reporting timeline that a small office would face. [Add two to four recent studies you have read yourself, with one line each on what they found and what they leave open.]

Bibliography

- Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., and Scarfone, K. (2016). *Guide for Cybersecurity Event Recovery* (NIST Special Publication 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., and Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1
- Indian Computer Emergency Response Team (2022). *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*, No. 20(3)/2022-CERT-In, 28 April 2022. Ministry of Electronics and Information Technology, Government of India.
- Government of India (2000). *The Information Technology Act, 2000* (Act No. 21 of 2000), section 43.
- School of Vocational Education and Training, IGNOU (n.d.; PDF file created March 2022). *MSEP-028/MSEP-038 Project Guidelines, MSCIS/PGDIS (Project-I and II)*.
- [Your own sources: author, year, title, publisher or journal, link.]

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION

The guidelines set no referencing style. Pick one style and use it the same way in every entry.

Before you send it

- Proforma (page 5) filled in full: course code, enrolment number, Study Centre, Regional Centre and RC code, e-mail, mobile, name and address, title; signed and dated by you.
- Proposal of about 15 pages covering all eight parts.
- Envelope marked: MSCIS/PGDIS Project Proposal (MSEP-028/MSEP-038).
- A photocopy of the whole packet kept with you (section V.5); our advice: keep the postal receipt or a receipt from the Study Centre too.

SAMPLE FOR STUDY REFERENCE, NOT FOR SUBMISSION