**A PROJECT REPORT**

**ON**

**“Cybersecurity Policy and Incident Response Plan for a Small Business”**

*United College of Engineering and Research, Prayagraj*

BACHELOR OF TECHNOLOGY (CSE)

Supervisor’s Name: Mr. Ayush Kumar

Submitted : Anuj Singh Yadav

**Date : July 31, 2025**

**Table of Contents**

1. Title page

2. ⁠Abstract

3. ⁠Table of Contents

4. ⁠Introduction

5. Literature Review

6.Methodology/Approach

7. Result and Discussion

8. Conclusion

9. Recommendations

10. References

11. Appendices

**Abstract**

This project presents a comprehensive cybersecurity policy and an incident response plan tailored for small businesses. Small businesses often lack the resources or expertise to manage complex IT infrastructures and are increasingly targeted by cybercriminals. This project outlines a simple yet effective policy to protect sensitive data and respond to security incidents efficiently. The policy includes sections on data protection, acceptable use, password guidelines, and access control. The incident response plan defines key roles, identifies incident types, and details a step-by-step response procedure. The goal is to provide an actionable framework that can be implemented even in businesses without dedicated IT personnel. The report discusses research findings, policy drafting techniques, challenges faced, and recommendations for future improvements.

**Introduction**

With the rising number of cyberattacks, small businesses are vulnerable due to limited resources for cybersecurity. This project focuses on creating a practical cybersecurity policy and an incident response plan that can be realistically adopted by small businesses. The objective is to provide a structured approach to preventing, detecting, and responding to cyber threats. This project uses real-world references, cybersecurity standards, and best practices to frame an easy-to-follow policy and response plan suitable for non-technical users.

**Literature Review**

Small businesses contribute significantly to the economy but often underestimate cybersecurity threats. According to recent research, over 60% of cyberattacks target small businesses. Frameworks like NIST and ISO/IEC 27001 have provided detailed guidelines, but they are often too complex for small firms. Simplified frameworks and case studies show that clear policies, staff awareness, and basic security controls can drastically reduce risk. Prior studies also highlight the importance of a documented and practiced incident response plan to minimize damage.

**Methodology/Approach**

The project followed a structured plan:

1. Researching common cybersecurity threats faced by small businesses.

2. Reviewing existing frameworks (NIST CSF, CIS Controls).

3. Drafting a cybersecurity policy with essential sections.

4. Designing an incident response plan based on industry practices.

Tools and References Used:

- NIST Cybersecurity Framework

- CIS Controls v8

- Microsoft Security Guidelines

- SANS Incident Handler’s Handbook

Step-by-Step Process:

- Identified key components of an effective security policy: access control, data protection, acceptable use, password policy, etc.

- Developed sample policy language adapted to small business environments.

- Designed an incident response process including preparation, detection, containment, eradication, recovery, and lessons learned.

- Created visual aids (flowchart and tables) to simplify understanding.

**Result and Discussion**

Results:

Cybersecurity Policy:

- Clearly defined roles and responsibilities.

- Acceptable Use Policy (AUP).

- Password and account security guidelines.

- Data backup and recovery strategy.

Incident Response Plan:

- Defined 6 key phases: Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned.

- Flowchart created for easier navigation of response steps.

- Sample forms for incident logging and post-incident review.

Discussion:

The drafted policy was designed to be easily adopted without requiring advanced technical knowledge. The response plan provides a step-by-step procedure that can be followed even by non-IT personnel. The main challenge was balancing technical completeness with simplicity and ease of use. Emphasis was placed on clarity, prioritizing high-risk areas, and encouraging ongoing employee awareness training.

**Conclusion**

The project successfully developed a basic cybersecurity policy and an incident response plan tailored to small businesses. The policy addresses core security concerns while the incident response plan empowers businesses to act swiftly during cyber incidents. Key learnings include the importance of user-friendly documentation and regular training. If further developed, the plan can be extended to include risk assessments, third-party security, and regulatory compliance guidance.

**Recommendations**

- Conduct regular staff training on cybersecurity awareness.

- Periodically review and update the policy and response plan.

- Perform basic internal audits to check compliance.

- Invest in affordable tools for antivirus, backup, and monitoring.

- Establish communication channels for reporting incidents promptly.

**References**

1. National Institute of Standards and Technology (NIST). "Cybersecurity Framework."
2. https://www.nist.gov/cyberframework  
   2. Center for Internet Security. "CIS Controls v8." https://www.cisecurity.org/controls/

3. Microsoft. "Small Business Security Guidance."

4. SANS Institute. "Incident Handler's Handbook."

5. Verizon. "Data Breach Investigations Report 2024."

**Appendices**

- Appendix A: Sample Cybersecurity Policy Document

- Appendix B: Sample Incident Report Form

- Appendix C: Incident Response Flowchart

**THANK YOU**