HackTech

Web Filter Policy

HT-ISMS-PL-18

CONFIDENTIALITY

Document Control

Document Title	Web Filter Policy		
Document ID	HT-ISMS-PL-18		
Document Type	Policy	Classification	Internal
Version	1.0	Release Date	
Author	Name		
	Designation		
Reviewer	Name		
	Designation		
Approver	Name		
	Designation		

Revision History		
Version	Revision Description	Release Date
1.0	Initial Release	

Document Distribution			
Name	Department	Designation	Company
	IT	System Admin	HackTech
	IT	Information Security	HackTech

Table of Contents

1. Introduction

The Internet presents significant opportunities along with potential risks, making it crucial for HackTech to safeguard its employees and organizational interests from harmful content.

2. Scope

This policy applies to all users of HackTech-provided devices and networks, including employees, contractors, suppliers, and third parties with access to HackTech systems.

3. Relevant Policies

This policy is supplementary to the following HackTech policies and procedures:

- Acceptable Use Policy

4. Web Filtering Objectives

Access to the Internet from HackTech devices will be monitored to minimize exposure to malicious content, even on networks beyond HackTech's direct control (e.g., remote work and mobile networks).

5. Blocked Website Categories

The Security Team & IT Team will maintain a list of blocked website categories, including but not limited to:

- Sites hosting malware or involved in phishing activities

6. Exceptions and Access Requests

Access to blocked websites for business-justified reasons may be permitted on an exception basis, subject to approval by management.

7. Web-Based Email and File Downloads

Access to web-based email services is permitted but should be used cautiously. File downloads of allowed types will be allowed, with uploads subject to HackTech's Data Leakage Prevention Policy.

8. Social Networking Sites

Access to social networking sites is generally prohibited under the HackTech Acceptable Use Policy, unless explicitly permitted for specific business purposes.

9. User Awareness and Training

All HackTech users will be informed that their Internet activity is monitored in accordance with this policy. Regular awareness training regarding online threats will be provided to enhance user understanding and compliance.

10. Logging and Monitoring

Attempts to access blocked websites continuously will be logged and may be included in management reports. Persistent attempts to access blocked content may result in disciplinary action.

11. Policy Amendments

Changes to web filtering policies within monitoring software will be managed through a formal change control process to ensure transparency and accountability.

12. Conclusion

Adherence to this policy is essential to uphold HackTech's commitment to maintaining a secure and productive work environment. Users are expected to familiarize themselves with this policy and comply with its provisions to mitigate risks associated with Internet usage.