HackTech

Threat Intelligence Procedure

HT-ISMS-SOP-37

CONFIDENTIALITY

This document is prepared by HackTech**.** All rights are reserved. No part of this document may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying without the written permission of HackTech. If this copy of the document is a hard copy, it is likely to be an obsolete version. Please check with the author of this document, to ensure that you are referring to the current version.

Document Control

Document Title	Threat Intelligence Procedure		
Document ID	HT-ISMS-SOP-37		
Document Type	Procedure	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
Employee 1	IT	System Admin	HackTech
Employee 2	IT	Information	HackTech

Table of Contents

1. Purpose

The purpose of this document is to outline the procedures for gathering, analyzing, disseminating, and utilizing threat intelligence within the organization. It is intended to support the organization's proactive security posture by identifying potential threats, vulnerabilities, and attack vectors, thereby enabling a timely response to mitigate risks.

2. Scope

This procedure applies to all employees of HackTech, and contactors and third parties involved in threat intelligence activities within the organization. It covers the entire lifecycle of threat intelligence, from planning and collection to dissemination and action

3. Roles & Responsibilities

Security Team

4. Threat Intelligence Sources

HackTech has registered themselves with some of the following sources to receive periodic updates and solutions on nature of threat

5. Handling Threat Data

- HackTech collects, analyses and classifies the threat data based on sensitivity (e.g., public, internal, confidential).

6. Dissemination

- Intelligence is shared within the organization by sending out emails at periodic intervals

7. Response to Threat Intelligence

- Threat intelligence is integrated with the Incident Response Team's processes to provide real-time context for investigations.

8. Training and Awareness

- The concerned stakeholders are regularly trained on how to interpret and use threat intelligence effectively.

9. References

- Vulnerability Management Policy