CYBER INCIDENT RESPONSE POLICY

Revised: Oct, 2023

Forty Five Positive Tech Pvt Ltd
B-904, Emaar Digital Greens, Sector-61, Gurgaon, Haryana 122102

Revision History

Version-1 (v1) Release	**Apr, 2021**
Version-2 (v2) Release	**Jun 2022**
Version-3 (v3) Release	**Oct 2023**

CYBER INCIDENT RESPONSE POLICY

1. PURPOSE

1.1. The aim of this Cyber Incident Response Policy ("**Policy**") is to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operations of M/s Forty-Five Positive Tech Private Limited ("**Company**"), operating under the brand name SPALBA, and a swift and complete response to any incidents is necessary in order to maintain that availability and protect the available information.

1.2. This Policy shall be read in conjunction with the Terms and Conditions and other policies of the Company, as have also been made available on the official website of the Company. In case of any article / clause / definition / provision which may not have been covered in this Policy, such article/ clause / definition / provision shall be applicable in conjunction with the instant Policy, as has been mentioned in the Terms and Conditions laid down by the Company.

2. SCOPE

The scope of this Policy is applicable to all Information Technology (IT) resources owned or operated by the Company. Any information, not specifically identified as the property of other parties, that is transmitted or stored on the Company IT resources (including e-mail, messages and files) is the property of the Company. All users of the Company's IT resources including but not limited to its employees, contractors, vendors or others are responsible for adhering to this Policy.

3. RESPONSIBLE EXECUTIVE

The Administration Head shall be the Responsible Executive. Such designation and authorisation of the responsible executive, may vary as per the sole discretion and decision of the management of the Company. The responsibilities of the Responsible Executive include, but are not limited to:

(i) Receiving initial notification and status reports from the Incident Response Manager, duly appointed by the management of the Company, for the purposes of this Policy.

(ii) Release a notification to Public, regarding involvement of the Company's attorney and notification to law enforcement.

(iii) Preparing and delivering requisite press releases, which shall be first approved and allowed by the management of the Company, in writing.

(iv) Updating appropriate staff on priorities for response and recovery.

(v) Advising the Incident Response Manager, duly appointed by the management of the Company.

4. INCIDENT RESPONSE MANAGER

The Company designated Incident Response Manager bears the responsibility for preparing and coordinating the response to a cyber incident. The responsibilities of the Incident Response Manager includes, but are not limited to:

(i) Training users to recognize and report suspected incidents annually or as needed.

(ii) Developing and testing response plans as and when needed and submit test results to Executive Management which is necessary for external compliance.

(iii) Ensuring correctness of the Incident Response Plans which are executed.

(iv) Being the point of contact for any employee / consultant / associate of the Company, should any employee / consultant / associate or official believes that an incident has occurred

(v) Direct the identified technical support to manage the cyber incident.

(vi) Notify the appropriate executives of the management of the Company in writing that a cyber-incident has occurred.

(vii) Advising executives and appropriate staff regarding notification of payment brands, law enforcement agencies.

(viii) Providing information to the individual(s) responsible for notifying the press and public.

(ix) Coordinating with respect to logging and documentation of the incident and response.

(x) Making recommendations to reduce number of same or similar cyber incidents.

(xi) Track incident response performance of all such cyber incidents and give a written report of the same to the management of the Company.

(xii) Update the Incident Response Plan/procedures as needed by the Company.

(xiii) Bear the responsibility for disseminating this Policy and its relevant procedures to the identified roles, so that the entire personnel of the Company is aware about such Policy.

5. TECHNICAL SUPPORT STAFF

The Company's operations team shall provide technical support to the Incident Response Manager. The responsibilities of the technical support staff shall include, but are not limited to:

(i) Assessing the situation and providing corrective recommendations to the Incident Response Manager.

(ii) Helping the Incident Response Manager in making initial response to such identified cyber incidents.

(iii) Responding to the incident to check and solve the problems.

(iv) Reporting to the Incident Response Manager on actions taken and progress on the cyber incident.

(v) Participating in review of the cyber incident and development of recommendations to reduce future exposure.

(vi) Consulting with other executives and appropriate staff on public notification, and notification to the law enforcement agencies.

(vii) Assisting with preparation of press releases.

(viii) Consulting with appropriate staff on priorities for response and recovery.

(ix) Advising the Incident Response Manager.

6. GENERAL EMPLOYEES

6.1. It is the responsibility of all the employees of the Company to adhere to all the corporate security policies and procedures. They are required to promptly report information to any security incidents to the Company's Incident Response Team for evaluation.

7. NOTIFICATION/REPORTING REQUIREMENTS

7.1. External communications to customers, law enforcement, press and attorneys are reviewed by executive management prior to submission.

7.2. Any cyber incident which can be termed as disaster will immediately trigger execution of the Disaster Recovery Plan.

7.3. Incidents of lesser severity require an immediate meeting of the Company's Incident Response Team and Management of the Company will be informed immediately.

7.4. Level 2 cyber incidents of even lesser severity will require a report to the Company's Incident Response Team and further review in the next scheduled meeting.

7.5. Incidents of very low severity will be included in monthly reports to the Company's Incident Response Team and Management.

7.6. The Incident Response Manager is responsible for reporting to any customers/external agencies, as may be approved with the prior written notification from the management of the Company.

8. TYPES OF INCIDENTS

The Company's Incident Response Team will classify all incidents into one of three types:

8.1. Disclosure Incidents:

Those incidents which, , require the Company to notify customers, law enforcement or examiners as a statutory compliance measure. The Company must comply with all the applicable laws and regulations, including state and central laws.

8.2. Security Incidents:

These are incidents related to the confidentiality and integrity of information. They can include but not limited to technical incidents such as malware (virus, worm, and Trojan horse) detection, unauthorized use of computer accounts and computer systems, non-technical incidents such as improper use of information assets.

8.3. Negative Incidents:

These are incidents related to the availability of information of assets or other risks such as but not limited to legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information unlicensed application on the Company's System that does not impact confidentiality, integrity, or availability, but this Policy still requires the company Incident Response Team to track it.

9. INCIDENT DETECTION

9.1. The primary means of detection of technological intrusion is to leverage a suite of tools that monitor network traffic, logs, processes, and various other information points to detect exploitation attempts. Alarms are generated *via* security system dashboard or automated alerts.

9.2. The Company's team members are trained to notify the Company's Incident Response Team at irt@spalba.com in the event that they detect a potential cyber security issue.

9.3. The Company's Incident Response Team generates a ticket and explores the issue to determine if it is a true incident or not.

10. RESPONSE METRICS

10.1. Below is a list of general metrics that will be captured during the Incident Response Process. The present list may be modified as required throughout the everyday operation process:

(i) Detection Time

(ii) Dwell Time

(iii) False Positive Rates

(iv) Percent of Incidents detected by automated tools

11. INFORMATION SPILLAGE DETECTION AND RESPONSE

11.1 The information owner will evaluate the report and delegate the appropriate personnel to coordinate and offer a remedy for such spillage of information. The information owner is responsible for putting in place controls that allow personnel to continue to perform their role despite the spillage of information.

11.2 The Incident Response Team will then isolate the system and contain to minimize the spillage and preserve evidence. Affected devices/systems must immediately take on the classification of the data that is spilled limiting exposure of unauthorized personnel to the data. Upon completion of investigation, the Incident Response Team will eradicate the data from the device/system.

12. INCIDENT RESPONSE TRAINING

12.1 The Incident Response Manager is responsible for conducting a gap analysis on the skills of the Incident Response Team with regard to the current threat landscape. Formal or informal training will be conducting to bridge the gap as needed. During employee annual reviews, an assessment of skills will be conducted and a path to increase the capabilities of the Incident Response Team personnel, will be outlined.

12.2 Training of incident response policy/procedures will be conducted during employee onboarding and also as and when needed.

13. INCIDENT RESPONSE TESTING

13.1 The Incident Response Manager builds and schedules the annual incident response exercise plans.

13.2 The Incident Response Manager is responsible for disseminating the test plan to execute management, third parties, and necessary personnel.

13.3 The tests are designed to baseline the response time of the Incident Response Team and validate that proper procedures are followed to minimize the Company's time to recover from a cyber-incident.