CYBER INCIDENT RESPONSE POLICY

1. PURPOSE

The aim of the policy is to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operation of WMW EVENTS & ENTERTAINMENT PRIVATE LIMITED (hereinafter the "Company") and a swift and complete response to any incidents is necessary in order to maintain that availability and protect information.

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 Mr. Ritesh Chadha shall be the Responsible Executive. The responsibilities of the executive include, but are not limited to:

i. Receiving initial notification and status reports from the Incident Response Manager
ii. Public notification, involvement of the organization's attorney and notification to law enforcement
iii. Preparing and delivering press releases
iv. Updating appropriate staff on priorities for response and recovery
v. Advising the Incident Response Manager on priorities

WMW Events And Entertainment Pvt. Ltd.
Authorised Signatory

4. INCIDENT RESPONSE MANAGER

The Company designated Incident Response Manager bears the responsibility for preparing and coordinating the response to a cyber incident. Responsibilities include, 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 and as necessary external compliance entities.
iii. Insuring incident response plans are executed correctly
iv. Being the point of contact should any employee or official believe an incident has occurred
v. Involving the identified technical support to address the incident
vi. Notifying the appropriate executives that an incident has occurred if significant
vii. Advising executives and appropriate staff regarding notification of payment brands, law enforcement agencies and the corporate attorney if appropriate
viii. Providing information to the individual (s) responsible for notifying the press and public
ix. Coordinating the logging and documentation of the incident and response
x. Making recommendations to reduce exposure to the same or similar incidents
xi. Track incident response performance
xii. Update the Incident Response Plan/Procedures as needed
xiii. Bear the Responsible for disseminating policy/procedures to identified roles.

5. TECHNICAL SUPPORT STAFF

The Company's operations team shall provide technical support to the Incident Response Manager. Responsibilities 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 make initial response to incidents
iii. Responding to the incident to contain and correct problems
iv. Reporting to the Incident Response Manager on actions taken and progress
v. Participating in review of the 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 on priorities.

6. GENERAL EMPLOYEES

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

7. NOTIFICATION/REPORTING REQUIREMENTS

External communications to customers, law enforcement, press and attorneys are reviewed by executive management prior to submission. Any incident which can be termed a disaster will immediately trigger execution of the Disaster Recovery Plan. Incidents of lesser severity require an immediate meeting of the Company's Incident Response Team and Management will be informed immediately. Level 2 incidents of even lesser severity will require a report to the Company's Incident Response Team and further review in the next regularly scheduled meeting. Incidents of very low severity will be included in monthly reports to the Company's Incident Response Team and Management. The Incident Response Manager is responsible for reporting to any customers/external agencies.

8. TYPES OF INCIDENTS

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

i. **Disclosure Incidents**:

WMW Events And Entertainment Pvt. Ltd.
Authorised Signatory

These are incidents which, because of some statute or regulation, require the Company to notify customers, law enforcement or examiners. Company must comply with all applicable laws and regulations, including state and central laws.

ii. **Security Incidents**:

These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and Trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets.

iii. **Negative Incidents**:

These are incidents related to the availability of information assets or other risks such as 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

i. 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

ii. The Company's Team members are trained to notify the Company's Incident Response Team at it.wmw@wemediaworks.com in the event that they detect a potential security issue.

iii. The Company's Incident Response Team generates a ticket and explores the issue to determine if it is a true incident.

10. RESPONSE METRICS

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:

- Detection Time
- Dwell Time
- False Positive Rates
- Percent of Incidents detected by automated tools

WMW Events And Entertainment Pvt. Ltd.
Authorised Signatory

11. INFORMATION SPILLAGE DETECTION AND RESPONSE

The Company has put in place automated systems capable of detecting sensitive information and alerting the Incident Response Team whenever sensitive data is transferred to unauthorized devices and systems. Upon detection, the Incident Response Team will assess if a spill has occurred and report the potential spillage to the information owner.

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. The information owner must assess if legal authorities needs to be involved.

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

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.

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

13. INCIDENT RESPONSE TESTING

The Incident Response Manager builds and schedules the annual incident response exercise plans. The Incident Response Manager is responsible for disseminating the test plan to execute management, third parties, and necessary personnel. The tests are designed to baseline the response time of the incident response team and validate that proper procedures are followed to minimize the organization's time to recover from an incident.

WMW Events And Entertainment Pvt. Ltd.
Authorised Signatory