MUSIC BROADCAST LIMITED

Risk Management Policy

1. Preamble

Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board of Directors laid at the general meeting shall include a statement on the development and implementation of a risk management policy for the company.

Section 177(4)(vii) of the Companies Act, 2013 provides that Audit Committee shall evaluate the internal financial controls and risk management systems of the company.

SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 as amended from time to time, require the top 1000 listed companies (by market capitalisation), mandates laying down the procedures for risk assessment and minimization.

Against this backdrop, Music Broadcast Limited ("MBL" or the "Company") has established this Risk Management Policy. This Policy lays down the principles and practices of the risk management system in MBL. The main principles of MBL's Risk Management are as follows:

- Develop risk awareness
- Focus on material risks and sources that threaten business objectives
- Focus on cyber security breach which include digital security breach or disruption to digital infrastructure, due to intentional or unintentional actions, such as cyber-attacks or human error. etc. Pro-active risk behaviour
- Dynamic, continuous risk assessment and responsiveness to changes
- Continuous ongoing process based on self-assessment

The main objectives of the Risk Management Policy are as follows:

- To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed.
- To establish a framework for the company's risk management process and to ensure companywide implementation.
- To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
- To assure business growth with financial stability.

2. Definitions

"Risk" *means* a negative effect of uncertainty on the achievement of business objectives.

Material risks arise when earning capacity is threatened or other important business objectives are prevented from being achieved. The framework of the Risk Management System is to ensure that the focus of the Company's business dealings is on optimizing the critical success factors for achieving the business objectives as defined in MBL's Operating Plan.

Mitigation: MBL continues to strengthen its responses to cybersecurity threats through proactive and reactive risk mitigations. These include,

Risk is characterized and rated by two factors:

- Impact
- Likelihood (L)

"Impact" is the potential damage/loss likely to be caused by a risk. The possible impacts can be subdivided into classes according to their severity.

"Likelihood" is the chance of something happening measured or determined quantitatively or qualitatively.

"Risk owner" is a person with the accountability and authority to manage an identified risk. All the Functional Heads shall be risk owners with regard to their respective areas of operation and the unit heads shall be the risk owners of units.

"Corporate Risk Coordinator (CRC)" is the person nominated by the Risk Management Committee and assigned with such responsibilities as mentioned in this policy. Presently, CEO has been nominated as CRC by the management.

3. Constitution of Risk Management Committee

Pursuant to Regulation 21 (5) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 as amended from time to time, the Company which is amongst top 1000 listed entities, based on market capitalization, a Risk Management Committee ("RMC") has been constituted of the Board. RMC is authorized to exercise the powers of the Board relating to monitoring and reviewing of the risk management plan specifically covering cyber security of the Company. The RMC powers and responsibilities are listed in Annexure 1.

The Risk Management Committee shall have minimum 3 members with majority of being the members of the Board of Directors including at least one independent director. Senior Executives of the Company may be members of the Committee but the Chairman of the Committee shall be member of the Board of Directors.

The Members of the Risk Management Committee are:

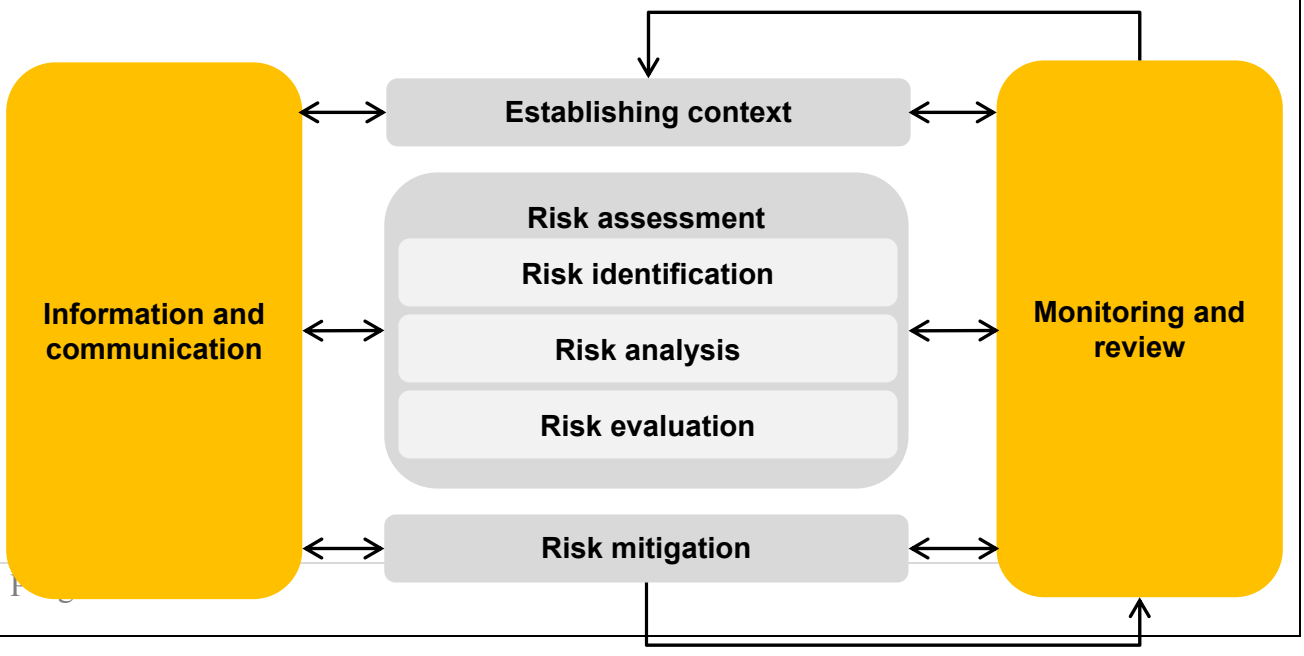
Sl. No.	Name	Designation
1.	Mr. Vijay Tandon, Chairman and Independent Director	Chairman of the Committee
2.	Ms. Anita Nayyar, Independent Director	Member of the Committee
3.	Mr. Ravi Sardana, Independent Director	Member of the Committee
3.	Mr. Ashit Kukian, CEO	Member of the Committee

The quorum for Risk Management Committee shall be one-third of its total strength or two members, whichever is higher, including at least one member of the board of directors in attendance. Risk Management Committee shall meet twice in a year with a gap between two meetings shall not be more than 180 days.

4. Overview of the Risk Management System at MBL

The basic principle for an effective risk management is the establishment and continuing evolution of appropriate risk awareness at all hierarchic levels of the organization. The early detection and cognizant handling of risk is the main objective of risk management. Explicit and effective risk management is a competitive advantage.

MBL has adopted the risk management process, comprising of five key activities as under



5. Roles and responsibilities in context of Risk Management (RM)

5.1 General roles and responsibilities within the Risk Management System

Board of Directors

The board of directors shall define the role and responsibility of the Risk Management Committee and the Committee shall be responsible to frame, implement, monitor and review the risk management plan and such other functions as Board may deem fit.

Risk Management Committee

The Risk Management Committee shall be responsible for framing, implementing and monitoring the risk management plan of the Company.

Audit Committee

The Audit Committee should ensure that adequate risk management systems exist. The Committee shall conduct thorough review of risk exposures on an annual basis.

Reporting, Controlling & Consolidation

The functional heads shall formally report to the CRC on risk management within their areas of operation. The purpose of this reporting is to assess how well "Key Risks" are managed and if any additional risk has emerged that can affect business operations. The risk report includes:

- Performance of functions in managing key risks in light of the mitigation strategies
- Identification of additions key risks that may have emerged including their mitigation strategies.

The results of this exercise shall be compiled by CRC and made available for review to the Risk Management Committee on half-yearly basis

5.2 Specific Roles and Responsibilities of the Management within the Risk Management System

Corporate Risk Coordinator (CRC)

The CRC is responsible for the risk assessment process throughout the functions, various units and market. CRC is also responsible to proactively ensure proper reporting, completeness and timely delivery of quantitative and qualitative information related to risk and its status.

Risk Owner

The Risk Owner(s) shall be responsible for the identification and assessment of risks. The risk owner(s) shall also be responsible for the realization of actions to manage the risks (avoid, minimize, transfer of risk to a third party, etc.).

6. Risk Management Process

The Risk Management process is an ongoing activity. The risk assessment has to be performed on a continuous basis in order to manage efficiently the exposures. The results of the assessment and measurement shall be documented annually by Risk Management Committee. It consists of a bottom up approach.

The Risk Management process involves the following phases:

- Risk identification and analysis
- Risk evaluation
- Risk mitigation
- Monitoring and reporting

Key questions that a risk owner must ask:

- What could happen (threat event)?
- If it happens, how bad could it be (threat impact – risk exposure)?
- How often could it happen (threat frequency / probability analyzed)?

Analyzing and assessing risks will answer these questions. The need for action depends primarily on the above assessment.

6.1 Risk Identification and Analysis

Risk is defined as the effect of uncertainty on business objectives. The purpose of risk management is to identify potential threats that may affect realization of the business objectives or priorities. An annual risk assessment exercise is conducted by the CRC to identify the applicable risks and update the risk profile of the company. This risk profile/library is revisited by Risk Management Committee to identify any new risk event that can adversely impact business objectives.

6.2 Risk Evaluation

The purpose of risk evaluation exercise is to identify and prioritize key risks which can adversely impact business operations of the company. Prior to initiating the annual risk prioritisation exercise, the Risk Management Committee shall seek feedback from CRC

and Risk Owner, as may be deemed appropriate by Risk Management Committee. The CRC also facilitates prioritization of risks using the risk prioritization criteria.

The company performs an inherent risk evaluation i.e. the impact and likelihood of occurrence is evaluated on the assumption that controls are not in existence. The tables below highlight the parameters to be used for risk evaluation:

Impact/ Consequence – Quantitative			
Score	**Description**	**Decrease in turnover***	**Decrease in EBITDA***
5	**Critical**	▸ Decrease in turnover of greater than 15%	▸ Decrease in EBITDA of more than 15%
4	**Material**	▸ Decrease in turnover up to 15%	▸ Decrease in EBITDA up to 15%
3	**Important**	▸ Decrease in turnover up to 10 %	▸ Decrease in EBITDA up to 10 %
2	**Moderate**	▸ Decrease in turnover up to 5%	▸ Decrease in EBITDA up to 5%
1	**Minor**	▸ Decrease in turnover up to 1%	▸ Decrease in EBITDA up to 1%

**Turnover is defined as gross turnover*

**EBITDA is defined as earnings before interest, taxes, depreciation and amortization*

Impact/Consequence – Qualitative		
Score	**Description**	Examples:
5	**Critical**	▸ Brand and reputational Impact such as Negative attention/ action from government agencies (EHS Laws & Regulations) Negative attention or actions from, consumers, Sustained Negative comments in the Social Media, cyber security breach which include digital security breach or disruption to digital infrastructure etc. ▸ Impact on Human Resources such as Loss of a significant number of key personnel; Sustained employee dissatisfaction, increase in attrition rate etc.
4	**Material**	
3	**Important**	

2	**Moderate**	▸ Impact on Business operations such as substantial loss of business capability; multiple fatalities of personnel; major IT system down, fatalities/disaster leading to regulatory intervention and possible radio station closure etc. ▸ Liabilities of directors due to non-compliances with laws and regulations leading to major penalties and severe imprisonment etc. ▸ Loss of market share due to failed innovations, increase in competition etc. ▸ Product quality having severe/major impact on listenership numbers.
1	**Minor**	

Probability/Likelihood of occurrence		
Score	**Rating**	**Probability/Likelihood of occurrence**
5	**Expected/ Almost Certain**	Very high, will be almost a routine feature every month/quarter within the immediate next 12 months
4	**Likely**	High, may arise several times within the next 12 months
3	**Possible**	Possible, may arise once or twice within the 12 months
2	**Unlikely**	May occur once or twice between year 2 (from now) to 3 years
1	**Rare**	Not likely, almost impossible to occur between year 2 (from now) to 3 years

The 'CRC' facilitates prioritization of risks using the above risk evaluation criteria annually. The results of the annual risk evaluation are subject to review, change and approval by the Risk Management Committee.

6.3 Risk Mitigation

Risk mitigation involves one or more options for the modification of the risk impact or the likelihood of the occurrence. When selecting the most appropriate risk treatment alternative, all costs and efforts of implementation should be balanced against the benefits derived.

Following steps are followed in identification and documentation of mitigation plans:

- The functional heads have the responsibility for the quality and completeness of the mitigation plans.
- CRC facilitates documentation of the mitigation plans and mapping the risk owners against key risks.
- All risk mitigation plans are submitted to CRC for review and approval and subsequently to Risk Management Committee for consideration.

6.4 Risk Monitoring

Risk monitoring involves monitoring the implementation and progress of agreed actions, re-evaluation, and compliance with decisions. The cost of controlling a risk may be taken into account in determining what is reasonably practicable and should not be used as a reason for not implementing the mitigating control.

In order to ensure that the implemented control measures remain effective, the following points should be considered:

- Clear accountability of responsibilities
- Effective communication of risk controls
- Regular review of proposed procedures
- Up to date training
- Up to date risk information and follow-up of changes in operating conditions

The Company acknowledges that despite best efforts by all concerned to manage risks there may be situations which need to be managed as a crisis by the top management.

7. Risk Reporting and Timetable

The risk reporting to be presented shall comprise of the following:

- **Half Yearly:** The CRC shall, on half yearly basis, follow-up the major risks and accordingly prepare and action for the same subject to approval of Risk Management Committee.

- **Incidental-Ad hoc risk reporting:** Functional Heads and Unit Heads are required to report ad hoc newly recognized, sudden and unexpected major risks (quantitative and qualitative) to the CRC. Ad hoc risk reporting is an important tool to avoid surprise losses and escalation of risk exposures.

  All risks related to fraud, corruption and anti-competition shall be reported ad-hoc, independently of the amount and the probability of occurrence.

**This Policy was approved by the Board of Directors at its Meeting held on May 20, 2021*

ANNEXURE-1

POWERS AND RESPONSIBILITY OF RISK MANAGEMENT COMMITTEE (RMC)

The RMC shall have the following powers:

1. To investigate any activity within its terms of reference.
2. To seek information from any employee.
3. To obtain outside legal or other professional advice.
4. To secure attendance of outsiders with relevant expertise, if it considers necessary.

The Committee shall have the following responsibilities:

1. To formulate a detailed risk management policy which shall include:
   (a) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
   (b) Measures for risk mitigation including systems and processes for internal control of identified risks.
   (c) Business continuity plan
2. To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company
3. Discuss with senior management, the Company's Risk Management System ("RMS") and provide oversight as may be needed.
4. Ensure it is apprised of the most significant risks along with the action management is taking and how it is ensuring effective RMS.
5. Reviewing risk disclosure statements in any public documents or disclosures.
6. Review and recommend changes to Risk Management Policy and / or associated frameworks / plans including cyber security, processes and practices of the Company.
7. Be aware and concur with the Company's risk appetite including risk levels, if any, set for financial and operational risks.
8. Ensure that the Company is taking appropriate measures to achieve prudent balance between risk and reward in both ongoing and new business activities.
9. Review the Company's portfolio of risks and consider it against the Company's risk appetite.
10. Being apprised of significant risk exposures of the Company and whether management is responding appropriately to them.
11. To keep the Board of Directors informed about the nature and contents of its discussions, recommendation and action to be taken.
12. The RMC shall have access to any internal information necessary to fulfil its oversight role.

13. To ensure that appropriate methodology processes and systems are in place to monitor and evaluate risks associated with the business of the Company
14. To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity.
15. The appointment, removal and terms of remuneration of the Chief Risk Officer, if any.
16. Perform such other activities related to this Policy as requested by the Board of Directors or as may be stipulated in any applicable provisions as amended from time to time or to address issues related to any significant subject within its term of reference