

**MAIL.RU GROUP LIMITED (THE “COMPANY”)  
RISK MANAGEMENT POLICY**

**Introduction**

As one of the leading companies in Russian-speaking segment of the Internet with business activities in several countries, Mail.ru Group Limited and its controlled subsidiaries (together, the “Group”) is exposed to a wide range of risks, some of which may have material consequences. The Group is subject to certain risks that affect our ability to operate, serve our clients, and protect our assets. These include, but are not limited to risks to employees, liability to others, and risks to property.

Controlling these risks through a formal program is necessary for the well-being of the Group as a whole and everyone in it individually. The jobs and services provided by the Group, the safety of the workplace and other benefits all depend to an extent on our ability to control risks.

The Group is committed to identifying and managing risk, in line with international best corporate governance practice.

Effective risk management allows us to:

- have increased confidence in achieving our goals
- manage risks at tolerable levels
- make informed decisions
- strengthen corporate governance procedures

**Responsibility**

- The board of directors (the “Board”) has a responsibility to ensure that it has dealt with the governance of risk comprehensively.



- The chief executive officer (CEO) is accountable to the Board for the enterprise-wide management of risk.
- Management is responsible for risk in accordance with approved plans and policies.
- The Risk committee assists the management in carrying out its responsibility for the governance of risk. A dedicated Risk manager reports to the Risk committee.
- The Risk committee advises on, formulates, implements and executes an adequate internal control framework and manages the risk management system and monitors the Group's risk profile, ensuring that major risks are identified and reported at the appropriate level within the Group.
- Internal audit provides assurance on the adequacy and effectiveness of the risk management process across the Group.
- The Audit committee assists the Board in its responsibility for overseeing financial reporting risks and internal financial controls, including fraud and IT risks as they relate to financial reporting, adequacy and effectiveness of risk management and addresses risk related issues as follows:
  - a. reviews and approves for recommendation to the Board a risk management policy and a plan developed by the management;
  - b. monitors implementation of the risk policy and plan, ensuring that the appropriate enterprise-wide risk management system and process is in place with adequate and effective risk management processes that include strategy, ethics, operations, reporting, compliance, IT and sustainability;
  - c. makes recommendations to the Board concerning risk indicators, levels of risk tolerance and appetite;

- d. monitors that risks are reviewed by management, and that management considers and implements appropriate responses to identified risks, so that they are managed within the levels of risk tolerance and appetite approved by the Board;
  - e. ensures that risk management assessments are performed regularly by management;
  - f. issues a formal opinion to the Board about the effectiveness of the system and process of risk management; and
  - g. reviews reporting concerning risk management that is to be included in the integrated report, ensuring it is timely, comprehensive and relevant.
- The Audit committee oversees the functioning of external and internal auditors, including satisfying itself that risks are assured through its review of the combined assurance model.

### **Scope and Revision**

The risk management policy is applicable to all operations where the Group directly or indirectly has more than 50% ownership and management control over operations.

The Board adopts a risk map, to be reviewed quarterly, for implementation of the risk plan. The risk map includes a description of risks, degree of gravity, risk owner/s and ways of mitigating the risks. The areas of risk focus for each reporting year are decided when the risk management plan is approved.

The policy is applicable to risks the Group faces in the execution of its strategy, operations, reporting and compliance activities and will be reviewed and updated as required.

## **Policy**

The Group maintains a transparent risk profile by using a structured, formal and planned approach to risk management. The identification, management and reporting of risks are embedded in its business activities and processes.

## **Framework**

The Group's enterprise-wide risk management (ERM) framework is designed to ensure that significant risks and related incidents are identified, documented, managed, monitored and reported in a consistent and structured manner across the Group. A common approach to risk analysis and management must be adopted across all areas of application. This framework sets out the minimum requirements for implementing the risk policy.

Sound risk management principles and practices will become an integral part of the normal management strategy for all departments within the Group. The management of risk will be integrated into existing strategic planning and operational process and is to be fully recognised in the funding and reporting processes.

Risk appetite (amount and type of risk that the Group is prepared to pursue, retain or take) will be set and reviewed by the executive management in consultation with the Board. Conflicting interests, for example where a business decision may exceed set risk appetite levels, will be dealt with by the Board.

The Group establishes Risk management committee (or Risk committee), comprised of the principal operating managers of the Group in order to manage the process. Committee's composition and responsibilities are documented in the Risk committee Charter.

## Managing Risk

Management, assisted by Risk committee, will analyse major inherent risks and implement effective mitigating strategies to reduce these to acceptable levels.

Risk committee and management will develop an annual plan to ensure that significant risks across the organisation are identified, documented, updated and reported.

The Risk committee will also work with management to update and document the policies, procedures and controls in place, whereby inherent risks are adequately managed and mitigated.

These could include, but are not limited to:

- Risk maps and registers
- Inherent and residual risk assessment
- Internal controls and procedures and the implementation of relevant policies
- Insurance and other forms of risk transfer
- Monitoring of risk, and
- Setting mitigation strategy

Internal audit is responsible for providing an independent written assessment to the Audit committee on the adequacy and effectiveness of the internal control environment implemented to manage inherent risk to an acceptable residual level.

Management, taking into account the opinion of assurance providers (e.g. internal audit), documents and reports residual risk to the Risk committee, specifically risks falling outside the risk tolerance of the Board.

## Reporting

Significant group-wide risks are recorded in a risk register and visualized on a risk map, along with their potential impact on the business and management's mitigating actions are documented.

The business units are required to identify such risks that they may be subject to, evaluate their impact on the business and document applicable risk management procedures in place. This risk information is reported to the Risk committee where the risks are evaluated and the risk register is updated as required.

Risk Management performance will be measured by a combination of:

- status of the risk register, extent to which risks are managed within the set appetite
- reporting on initiatives planned / completed that address exposures
- quarterly report on the performance in relation to the risk management objectives
- regular reports on incidents and accidents
- review of trends of key risk indicators, and
- risk owners are clearly identified

Risk register is amended on a semi-annual basis – at the time of approval of the annual business plan and 6 months thereafter.

We accept that risk management, including risk reporting, is a continuous process and will be improved as opportunities arise.

The risk reporting process is aligned with the Board's calendar.