ZEE ENTERTAINMENT ENTERPRISES LIMITED

INFORMATION SECURITY POLICY

Table of Contents

INTRODUCTION

At Zee Entertainment Enterprises Ltd., we are committed to providing high-quality entertainment and OTT services while upholding the highest standards of information security. We recognize the importance of protecting our customers' and stakeholders sensitive data and maintaining the trust they place in us. As part of our commitment to Information security and privacy, we have implemented the ISO 27001: 2013 framework and diligently practice information security throughout our organization.

Our Information Security Management System (ISMS) is designed to safeguard the confidentiality, integrity, and availability of our customers' and stakeholders information. We have established a robust set of controls and procedures to manage and mitigate information security risks effectively.

KEY PRINCIPLES

Confidentiality

We ensure that our customers' data remains confidential and protected from unauthorized access or disclosure. We have implemented stringent access controls, encryption mechanisms, and employee training programs to maintain the confidentiality of sensitive information.

Integrity

We maintain the integrity of our customers' data by ensuring its accuracy, completeness, and reliability. We have implemented data validation measures, secure storage mechanisms, and data backup procedures to prevent unauthorized modifications or data loss.

Availability

We strive to provide uninterrupted access to our services and platforms. We have implemented redundant systems, disaster recovery plans, and robust network infrastructure to minimize service interruptions and ensure our customers can enjoy our offerings without interruption.

GOVERNANCE STRUCTURE

Our information security practices are governed by a robust structure that ensures accountability and oversight. The governing structure consists of heads of all business units and functions within our organization. The governance structure ensures that information security responsibilities are well-defined, communicated, and effectively supported and executed across the organization.

INFRASTRUCTURE SECURITY

We follow a baseline security standard for all new IT infrastructure deployments. This ensures that all new systems are built with a strong foundation of security controls. We also perform regular Vulnerability Assessments (VA) across our infrastructure to proactively identify and remediate any potential vulnerabilities, ensuring a secure environment.

APPLICATION SECURITY

We conduct comprehensive Application Security Testing for all new applications before they are moved into production. This testing allows us to identify and address any security weaknesses or vulnerabilities early in the development lifecycle. Additionally, we undertake regular application security testing to identify and remediate new emerging vulnerabilities to ensure ongoing security posture.

CHANGE SECURITY GOVERNANCE

We recognize that any change to our information systems, applications, infrastructure, and business or operational processes can impact information security. Therefore, we have established a robust Change Security Governance framework to manage and control changes effectively. This framework ensures that security considerations are thoroughly evaluated and incorporated into the change management process. It includes comprehensive risk assessments, testing procedures, and stakeholder engagement to ensure that changes are implemented securely and do not introduce vulnerabilities or compromise the confidentiality or integrity of our systems.

SUPPLY CHAIN SECURITY

We understand that the security of our customers' data is not limited to our internal systems and processes. It extends to our relationships with external vendors and partners. To ensure the highest level of supply chain security, we undertake rigorous vendor risk management practices throughout the entire lifecycle i.e. Prior, during and at the time of termination of engagement.

COMPLIANCE

We comply with applicable laws, regulations, and industry standards relating to information security and privacy. Our ISMS framework aligns with the ISO 27001 standard, and we regularly assess and enhance our practices to stay current with emerging threats and evolving regulatory requirements.

EMPLOYEE AWARENESS

We believe that our employees play a vital role in maintaining information security. We provide regular training and awareness programs to educate our employees about their responsibilities, best practices, and emerging threats, ensuring that they are equipped to protect our customers' data effectively.

INCIDENT REPORTING

An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of ZEEL.

Any incident where an employee has a reasonable belief that there is a risk to the security of sensitive personal data, or any confidential information shall be reported.

The term security incident covers a wide range of events, that varies considerably. Following are examples for security incidents that shall be reported.

Type of data	Example
Sensitive personal data	Risk of accidental or deliberate disclosure of sensitive personal data.
Confidential information:	Risk of accidental or deliberate access of confidential information by an unauthorized person. e.g., Commercial data sent to the wrong recipient or information sent by email without password protection.
Passwords	An unauthorized person has gained access to your account or attempted to gain access using your password e.g., Password/login details left accessible and unsecured to visitors in home worker's home.
IT security breach	Degraded IT system integrity or loss of system availability posing threat to loss of information or disruption of activity
	Unauthorized access to data
Physical security breach	Unauthorized access to secure areas containing confidential information e.g., forced access to a locker containing confidential information or sensitive personal data
Theft or loss of portable media	Unencrypted laptops/portable media containing confidential or sensitive personal data lost or stolen. e.g. laptop stolen from car

An actual exposure or potential breach of sensitive personal data or confidential information, which may compromise the confidentiality, integrity or availability of information stored, processed, and communicated (i.e., hard copy or electronic format) shall be reported as a security incident.

Personnel shall take responsibility of ZEEL's assets and any loss of information. It is personnel's responsibility to notify the Information Security Team and local ZEEL IT Team immediately of any evidence or suspicion of any security violation.

BUSINESS CONTINUITY MANAGEMENT

Business continuity Management is crucial for ensuring the resilience of information security in the face of potential disasters. To achieve this:

a. Processes for information security continuity must be established, regularly tested, reviewed, and updated. Controls should be periodically tested and updated to meet continuity objectives during disruptions. Information processing facilities need redundancies to meet availability requirements.

b. Business continuity and disaster recovery arrangements are essential, requiring establishment, maintenance, and regular reviews to enhance resilience and response capabilities. Resources, including personnel and equipment, must be assessed for incident stabilization.

c. Communication with public safety services is vital, understanding their response time, knowledge of the organization's facility, and capabilities for emergency stabilization.

CONTINUOUS IMPROVEMENT

We are committed to continuous improvement in our information security practices. We regularly conduct risk assessments, internal audits, and vulnerability scans to identify areas for improvement and promptly address any potential vulnerabilities or weaknesses.

By adopting the ISO 27001 framework and implementing an effective ISMS, we demonstrate our dedication to information security and our commitment to our customers' privacy. We understand the trust our customers place in us, and we continuously strive to earn and maintain that trust by safeguarding their information.

POLICY COMPLIANCE & DISCIPLINARY ACTIONS

All personnel (employee, interns, retainers, suppliers, contractor, or consultant etc.,) using ZEEL's information assets shall comply with the Information Security Policy.

Information processing resources shall be used in accordance with the Information Security Policy. Disciplinary action shall be taken for any non-compliance (intentional or unintentional violation) to the Information Security Policy.