BOBCARD LIMITED

IT Outsourcing Policy

(Policy & Procedure)

Version: 1.1

(Approved by board in meeting held on 20/01/2025 Agenda item no 153/5D)

IT Outsourcing Policy & Procedure

DOCUMENT INFORMATION

DOCUMENT INFORMATION	
Policy Name:	Outsourcing Policy & Procedure
Policy Owner	CIO
Document Version No.	1.1
Document Version Date:	26-08-2024
Prepared By:	Mr. Niraj Yewlekar & Mr. Rahul Jadhav
Approved By:	Mr. Ayaskant Mohapatra
Informed and approved:	TMSC
Date of approval	19-12-2024 (Approved by Board on 20-01-2025)

REVISION HISTORY

Revision HISTORY Ver. 1.1			
Sr. No.	**Version No**	**Date**	**Section Addition**
1	1.0	01-10-2023	Initial Document
2	1.1	26-08-2024	Proposed changes updated in below

			table

VERSION HISTORY

Version HISTORY Ver. 1.0			
Sr. No.	**Version No**	**Date**	**Approved By**
1	1.0	31-10-2023	Board
2	1.1	19-12-2024	TMSC

REVISION HISTORY

S.No.	Clause/ Para No.	As per existing Policy	Proposed Change	Reason for Changes
1.0	All sections	Initial Version	Initial Version	Initial Version
1.1	Section 7.1	New Addition	Choosing an outsourcer - The criteria for selecting an outsourcer, including factors like reputation, service quality, staff competence, financial stability, employee retention, security standards, and compliance reports (e.g., SOC2 Type2, PCI DSS), shall be defined and documented, with further	Enhancement As per ISO 27001

			information security criteria based on risk assessment, and a written agreement ensuring compliance with PCI DSS requirements and clear delineation of responsibilities.	
	Section 7.2	New Addition	Assessing outsourcing risks - The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if BOBCARD will benefit overall by outsourcing the function to the outsourcer, considering both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g., if the controls necessary to manage the risks are too costly), the function shall not be outsourced.	Enhancement As per ISO 27001
	Section 7.3	New Addition	Contracts and confidentiality agreements - Legal, regulatory, and third-party obligations, including data protection/privacy laws and anti-money laundering requirements, as well as information security obligations and controls such as policies, background checks, access controls, incident management, asset return/destruction, intellectual property protection, security controls for IT systems,	Enhancement As per ISO 27001

			anti-malware measures, and IT change/configuration management, must be clearly defined and adhered to in the outsourcing agreement.	
	Section 7.4	New Addition	Hiring and training of employees - Outsourced employees, contractors, and consultants working directly or on behalf of BOBCARD shall undergo background checks equivalent to those conducted on BOBCARD employees, and all personnel, including third parties, shall receive suitable information security awareness, training, and education to clarify their responsibilities regarding BOBCARD's policies, standards, procedures, guidelines, and contract-defined obligations.	Enhancement As per ISO 27001
	Section 7.5	New Addition	Access Control - Access controls for BOBCARD shall include user identification and authentication, role-based authorization, data encryption in line with BOBCARD's policies, audit logging of access attempts with alarms for violations, and documented procedures on access control components like strong passwords, logical access rights, and regular reviews; physical access controls shall include layered barriers, strong facilities, key	Enhancement As per ISO 27001

			management, access logging, and intruder alarms; if hosted at a third-party data center, the operator must ensure physical and logical isolation of BOBCARD's assets, and all information assets must be retrieved or destroyed at the contract's termination, with formal accountability for highly classified assets.	
	Section 7.6	New Addition	Security Audits - BOBCARD shall periodically audit the outsourcer's physical premises for compliance with security policies and contract requirements, assess service levels to ensure they are consistently met, and review necessary controls to address any discrepancies, with the audit frequency determined by management based on recommendations from Internal Audit, Information Security, and Legal functions.	Enhancement As per ISO 27001

LIST OF ABBREVIATION:

Acronym	Description
CISO	Chief Information Security Officer

IT Outsourcing Policy & Procedure

Contents

IT Outsourcing Policy & Procedure

1. Introduction

BOBCARD's outsourcing policy emphasizes careful consideration and due diligence in enhancing efficiency. Proposals require thorough cost-benefit analysis and board approval based on clear business cases and security considerations. Senior Management retains ultimate responsibility for risk management, with defined policies, contingency plans, and exit strategies. Formal agreements, including NDAs and SLAs, ensure risk management and confidentiality protection. Outsourcing agreements with controls safeguard assets and customer interests, while regular monitoring and audits maintain information security and service levels.

2. Objective

The outsourcing policy aims to streamline the evaluation, selection, and management of outsourcing initiatives, optimizing operational efficiency and service quality while mitigating associated risks. It ensures alignment with organizational goals, regulatory compliance, and accountability throughout the outsourcing lifecycle, fostering cost-effectiveness, innovation, and sustained competitive advantage. This policy shall be made available to interested parties to protect BOBCARD's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy shall be documented and made available as documented information to all employees, contractors, partners, and other relevant stakeholders and effectively communicated within the organization. Continuous improvement of our Outsourcing policy is integral to our commitment to safeguarding sensitive data against evolving threats.

3. Scope

This policy applies to all organizational IT systems, networks, devices, and data assets, including desktops, servers, mobile devices, and cloud platforms. It covers all personnel and third-party entities accessing or managing these resources. The policy includes measures for antivirus software deployment, regular malware scanning, incident response protocols, and employee training.

4. Policy Statement

This policy governs all outsourcing activities within BOBCARD, covering IT services, customer support, procurement, and administrative functions. It applies to all departments, employees, and third-party service providers involved in outsourcing, managing the entire lifecycle from evaluation to termination. The policy includes guidelines for risk assessment, compliance management, and stakeholder communication to ensure alignment with organizational objectives and regulatory requirements.

5. Roles and Responsibilities

Roles	Responsibilities
IT Head	• Identify with the assistance of the IT Department, and list, the IT process / sub-processes and activities that are proposed to be outsourced. • list out the criteria for selection of the activity and the service providers for outsourcing. Parameters for defining Material Outsourcing, delegation of authority based on the risks and systems to monitor & review the operations of these activities shall also be listed out.

6. Standards Addressed

1. ISO 27001:2022 Controls
    - 5.2 - Policy
    - 10.1 - Continual Improvement
    - 5.3 - Organizational roles, responsibilities, and authorities

2. ISO 27002:2022 Controls
    - 5.19 - Information security in supplier relationships
    - 5.20 - Addressing information security within supplier agreements
    - 8.30 - Outsourced development

7. Security Controls

7.1 Choosing an outsourcer

1. Criteria for selecting an outsourcer shall be defined and documented, considering the: a) Company's reputation and history.
2. Quality of services provided to other customers.
3. Number and competence of staff and managers.
4. Financial stability of the company and commercial record.
5. Retention rates of the company's employees.
6. Quality assurance and security management standards currently followed by the company (e.g., certified compliance with ISO 9000 and ISO/IEC 27001).
7. Compliance reports like SOC2 Type2 reports and PCI DSS certificate of compliance (COS) annually.

   Further information security criteria shall be defined as the result of the risk assessment.
8. Maintain a written agreement that includes an acknowledgment from the service providers that they will comply with all applicable PCI DSS requirements. This applies to any service provider that handles, accesses, stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of the customer.
9. Keep accurate records specifying which PCI DSS requirements are managed by each service provider and which are the responsibility of the entity. This ensures clear delineation of compliance responsibilities and facilitates effective management of the overall security posture.

7.2 Assessing outsourcing risks

Management shall nominate a suitable owner for each business

function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using BOBCARD's standard risk assessment processes. In relation to outsourcing, specifically, the risk assessment shall take due account of the:

a. Nature of logical and physical access to information assets and facilities required by the outsourcer to fulfill the contract.

b. Sensitivity, volume, and value of any information assets involved.

c. Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to BOBCARD's competitors where this might create conflicts of interest.

d. Security and commercial controls are known to be currently employed by BOBCARD and/or by the outsourcer.

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if BOBCARD will benefit overall by outsourcing the function to the outsourcer, considering both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g., if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

7.3 Contracts and confidentiality agreements

1. A formal contract between BOBCARD and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing. If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between BOBCARD and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which shall be required before the main contract is negotiated). Information shall be classified and controlled in accordance with BOBCARD policy. Any information received by BOBCARD from the outsourcer

who is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling. Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality must be extended beyond the tenure of the contract. All contracts shall be submitted to the Legal for accurate content, language, and presentation.

2. The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions, or services being provided (e.g., defined service levels), liabilities, limitations on use of sub-contractors, and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:

    a. Legal, regulatory, and other third-party obligations such as data protection/privacy laws, money laundering, etc.

    b. Information security obligations and controls such as:

        i. Information security policies, procedures, standards, and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001.

        ii. Background checks on employees or third parties working on the contract.

        iii. Access controls to restrict unauthorized disclosure, modification, or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating, and revoking access to systems, data, and facilities, etc.

        iv. Information security incident management procedures including mandatory incident reporting.

        v. Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity.

        vi. Copyright, patents, and similar protection for any intellectual

property shared with the outsourcer or developed during the contract.

vii. Specification, design, development, testing, implementation, configuration, management, maintenance, support, and use of security controls within or associated with IT systems, plus source code return.

viii. Anti-malware, anti-spam, and similar controls.

ix. IT change and configuration management, including vulnerability management, patching, and verification of system security controls prior to their connection to production networks.

7.4 Hiring and training of employees

1. Outsource employees, contractors, and consultants working directly or on behalf of BOBCARD shall be subjected to background checks equivalent to those performed on BOBCARD employees.
2. Suitable information security awareness, training, and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to BOBCARD information security policies, standards, procedures, and guidelines (e.g. privacy policy, acceptable use policy, the procedure for reporting information security incidents, etc.) and all relevant obligations defined in the contract.

7.5 Access controls

1. To prevent unauthorized access to BOBCARD's information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design suitable controls architecture. Technical access controls shall include:
    a. User identification and authentication.

b. Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls.

c. Data encryption in accordance with BOBCARD's encryption policies and standards defining algorithms, key lengths, key management, and escrow, etc.

d. Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

e. Procedural components of access controls shall be documented within procedures, guidelines, and related documents and incorporated into awareness, training, and educational activities. This includes:

f. Choice of strong passwords.

g. Determining and configuring appropriate logical access rights.

h. Reviewing and if necessary, revising access controls to maintain compliance with requirements.

Physical access controls shall include:

a. Layered controls covering the perimeter and internal barriers.

b. Strongly constructed facilities.

c. Suitable locks with key management procedures.

d. Access logging using automated key cards, visitor registers, etc.

e. Intruder alarms/alerts and response procedures

If parts of BOBCARD's IT infrastructure are to be hosted at a third-party data center the data center operator shall ensure that:

a. BOBCARD's assets are both physically and logically isolated from other systems.

b. BOBCARD shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or

destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

7.6 Security audits

If BOBCARD has outsourced a business function to an outsourcer based at a different location:

1. It shall audit the outsourcer's physical premises periodically for compliance with BOBCARD's security policies, ensuring that it meets the requirements defined in the contract.
2. The audit shall also take into consideration the service levels agreed in the contract, determining whether they have been met consistently and reviewing the controls necessary to correct any discrepancies.
3. The frequency of audit shall be determined by management on advice from functions such as Internal Audit, Information Security Management, and Legal.

7.7 Policy Exception

In instances where deviations from this policy are necessary, a formal exception request must be submitted to the designated authority within the organization. The request should provide a comprehensive rationale for the exception, outline associated risks, and propose mitigation strategies. All exception requests will undergo a review process and require approval from TMSC. Once approved, exceptions will be documented and subject to periodic review to ensure ongoing alignment with organizational objectives and compliance with regulatory standards.

7.8 Policy Violation

1. All users shall read and abide by this Outsourcing Policy.
2. Violations of the Outsourcing Policy shall result in disciplinary action, up to and including termination of employment, depending on the severity and recurrence of the breach, ensuring accountability and deterrence against non-compliance.

7.9 Policy Review

The policy shall be reviewed for updates by CISO and approved by TMSC on an annual basis. Additionally, the policy shall be updated in-line with any major changes within BOBCARD's operating environment or on recommendations provided by the internal/external auditors.

---------- End of Policy and Procedure ----------