SOCIAL PILLARS

Consumer Protection

The Bank Operational Policy of Bank Mandiri governs the execution of consumer protection functions. Subsequently, internal policies within each work unit further elaborate on this policy. This demonstrates the Bank's commitment to support a reliable consumer protection system and achieve a financially sustainable, sound system that safeguards the interests of the public and consumers.

Since October 2022, Bank Mandiri has also established a Consumer Protection Unit as mandated by OJK Regulation No. 6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector, which is responsible for:

1. Disseminate the principles of Consumer Protection to all PUJK Employees.
2. Coordinate the planning and implementation of PUJK compliance with Consumer Protection provisions.
3. Coordinate monitoring and evaluation of the implementation of PUJK compliance with Consumer Protection provisions.
4. Report on implementation and provide recommendations to the Board of Directors related to Consumer Protection.
5. Coordinate the preparation and submission of reports related to Consumer Protection.

In addition to having a consumer financial protection policy, Bank Mandiri also has a debt collection policy that contains the fulfillment of debtor rights as stated in:

1. Bank Mandiri's Credit Policy with the latest amendments was signed by the Board of Directors and is effective as of 7 March 2022.
2. Standard Credit Collection & Recovery Operating Procedures as last amended in 2022.
3. Other related internal regulations

The regulation generally upholds debt collection procedures while safeguarding the welfare of debtors as consumers. When a Collection Service Provider Company handles the collection, Bank Mandiri shall ensure the following:

1. Collection can only be done if the quality of the debtor's receivables is included in the bad quality.
2. Informing the debtor if the collection of the debtor's obligations has been submitted to the Collection Service Provider Company.
3. Collection is prohibited by using physical or verbal pressure;
4. Collection is prohibited from being made to parties other than the debtor;
5. Collection using means of communication is prohibited from being continuously disruptive;
6. Collection can only be done at the place of the debtor's billing address or domicile;
7. Collection can only be done from 08.00 to 20.00 time in the debtor's domicile area.

In addition, the policy also regulates the rights of creditors to:

1. Obtaining a sufficient explanation of the characteristics of the product.
2. Access the terms and conditions of fund products through the Bank Mandiri website.
3. Obtain transaction convenience through branches, e-banking services or other facilities determined by the Bank.
4. Earn interest in accordance with the applicable provisions at the Bank.
5. Obtain information on procedures for handling and resolving customer complaints.

In the lending process, Bank Mandiri prioritizes the principle of prudence and regular portfolio monitoring. The application of the due-diligence in the lending process is reflected in the escalation mechanism in the loan approval and monitoring process for large-scale and high-risk debtors.

The lending process flow of the Loan Monitoring Stage includes the Watchlist mechanism as one of several methods for assessing the creditworthiness of existing debtors. This mechanism functions as an Early Warning Signal to assess the credit quality extended by examining three key factors: the debtor's future

business prospects, financial performance, and repayment history.

In the event that a decline in quality is detected during the review process, Bank Mandiri will intervene to rescue non-performing loans. An initiative undertaken by the Bank to address non-performing credit debtors who maintain viable business prospects and performance, and ability to repay, with the aim of minimizing the possibility of losses for the Bank and instill confidence in the lending.

The loan rescue may involve restructuring. The following restructuring measures may be implemented:
1. Reduction in lending rates;
2. Extension of credit term;
3. Reduction of credit interest arrears;
4. Reduction of credit principal arrears;
5. Additional credit facilities; and/or
6. Conversion of credit into temporary capital participation,

Bank Mandiri has also established the Business Committee and Risk Management & Credit Policy Committee, both of which are tasked with evaluating the Bank's products and services, including providing risk assessments of products and services issued by Bank Mandiri.

A complete review of the Business Committee and the Risk Management & Credit Policy Committee is detailed in the Bank Mandiri Annual Report, Corporate Governance Chapter, the Committee of the Board of Directors.

Bank Mandiri internal regulations govern marketing activities, communication, products, and services. This provision pertains to guidelines and standards for communication materials intended for public dissemination, with guidance and attention to regulatory regulations, such as POJK No.6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector and OJK Financial Services Advertising Guidelines. Consequently, published communication materials are also pay attention to the interests of consumers/customers. In its implementation, all Product and Service Marketing Communication activities are reported periodically to the Board of Directors.

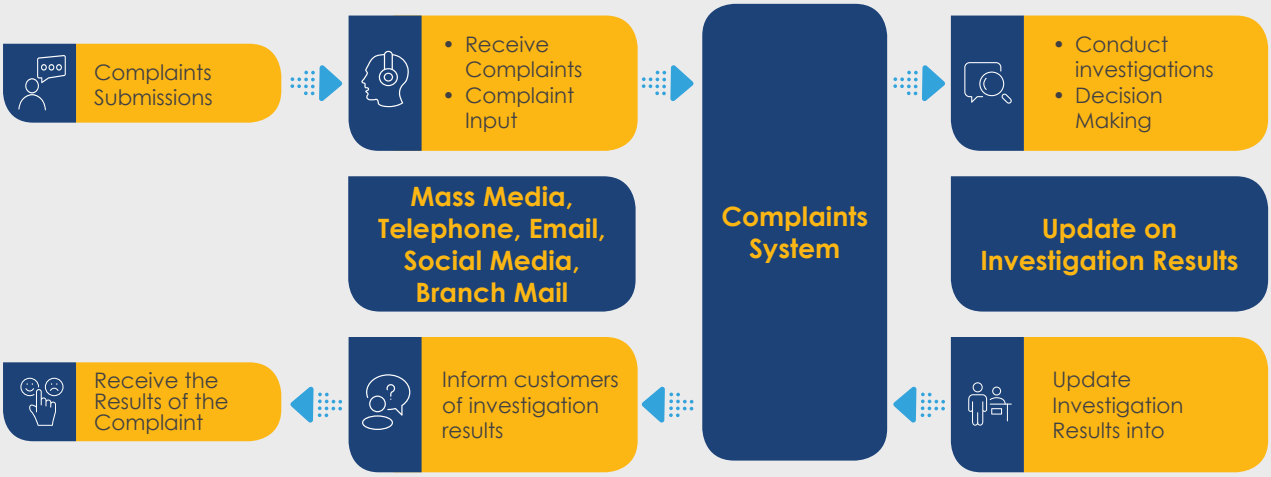
Bank Mandiri manages several financial literacy programs to improve people's financial literacy regarding finance and banking. Some of these programs are:
1. MSME Education on Livestock – "Seizing Business Opportunities for the Laying Chicken Farm Ecosystem"
2. MSME Education to Support Infrastructure Development
3. Mandiri Education
4. Education and Socialization of Tabungan Simpanan Pelajar (SIMPEL) and One Account One Student Program (KEJAR)
5. Financial Management and Planning for Payroll Customers
6. Personal Finance Webinar
7. Empowering Indonesian Migrant Workers through the Mandiri Sahabatku entrepreneurship program.
8. Financial Literacy Program (SME Group)
    - Mandiri UKM Center (UKMC) is a business model targeted to comprehensively work on the business potential of SMEs regulated within a certain radius, particularly in cities contributing to Indonesia's GDP (Gross Domestic Product).
    - Mandiri UKMC aims to provide a forum for MSME communities to obtain faster and easier credit financing and improve the competence of MSME communities through literacy mentoring/training, such as tax advisory, financial statement education, etc.

Bank Mandiri also conducts various trainings to improve the ability of employees in providing consumer protection which information is detailed in the Bank Mandiri Annual Report and Sustainability Report, Human Resources Chapter.

SOCIAL PILLARS

Moreover, Bank Mandiri has a complaint submission mechanism if customers experience problems in transactions, complaints or other complaints. Bank Mandiri established a special work unit, namely Customer Care Group to provide the best service. The main task of this unit is to resolve all customer complaints in accordance with the Service Level Agreement (SLA) that has been set.

CUSTOMER COMPLAINTS HANDLING



Customers are given easy access to complaint services with various media choices both oral and written, such as the following:

24 hours via Line
14000

Twitter Account
@mandiricare
and @bankmandiri

Livechat Whatsapp
0811-8414-000

Website
by selecting the "Contact us" menu.

Akun Facebook
"Mandiri Care" dan "Bank Mandiri"

An official letter addressed to Bank Mandiri, either delivered directly, or sent by post.

Email:
mandiricare@bankmandiri.co.id.

Instagram Account
@bankmandiri

Bank Mandiri throughout Indonesia.

Bank Mandiri also provides a whistleblowing system called Letter to CEO (LTC) in addition to the mechanism mentioned above. LTC is managed by an independent third party with the following objectives:

1. Be independent and professional.
2. Minimize the risk of conflict of interest.
3. Provide a sense of security for the whistleblower.
4. Increase stakeholder confidence in LTC management.
5. The whistleblower can monitor the follow-up status of the LTC report submitted.

Complete information on whistleblowing systems and mechanisms is detailed in this Annual Report - Governance Chapter, and Sustainability Report - Customer Service and Satisfaction Chapter.

Data Privacy and Security

Bank Mandiri sets priority on maintaining customer data privacy as part of human rights (HAM). We safeguard customers' personal information through technological, process & administrative, organizational and physical security steps. We develop code of ethics/business conduct including standards on how employees must protect customer confidential information.

Therefore, since customers open an account in Bank Mandiri Group, customers require to fill and check customers' consent according to the applicable regulations. Customers are also allowed to withdraw consumer's consent at any time. Furthermore, Bank Mandiri requires Non-Disclosure Agreement (NDA) for third party if there is cooperation that uses customer data, and only sends customer data according to customer's consent. The bank also ensures that delivery of campaign covering customer's consent.

The governance of customer data management has been formed in operational policies, namely Standard Data Management Procedures and Operational Technical Guidelines for the provision of internal and external data. Further information regarding the privacy policy and data security (including our subsidiaries) can be accessed through:

SOCIAL PILLARS

Mandiri Group are committed to building and updating reliable cybersecurity defense trough developing security requirement standards as a reference for each subsidiary based on Bank Mandiri's Cybersecurity Framework. Each Subsidiary will conduct self-assessment and prepare an action plan for compliance if there are any gaps with assistance by CISO Division. Furthermore, the action plan of each subsidiary is reported to Bank Mandiri's Management by Board of Directors of Subsidiaries to getting feedback to adapting the cybersecurity defense in Mandiri Group.

In addition, in order to perform the data harmonization process in the Subsidiaries, including data privacy and security, Mandiri Subsidiary Management Principle Guideline (MSMPG) has regulated provisions on data management that can be adopted and harmonized by the Subsidiaries. Issues and discussion topics related to data management, including data privacy and security, are reported and discussed at the board-level committee, namely the Data Steering Forum. The Data Steering Forum is held at least once a year attended by the Director of Risk Management, Director of Compliance, Director of Finance and Strategy, and Director of IT.

Regarding the management of confidentiality and security of personal data, Bank Mandiri has acquired and implemented a Data Governance Framework adopted from the best practice framework. Some of the practices include:

1. Customers can add/complete and change (rectify, change, control) personal data through branches or call centers.
2. The process of masking on sensitive data.
3. Protection of sensitive data against access by unauthorized parties/persons through the application of data classification.
4. Safeguarding against data leakage through the implementation of Data Loss Prevention (DLP) tool.
5. Secure file sharing with the implementation of multi-factor authentication (MFA) integrated into data management technology.
6. Periodic Security Awareness to educate employees and customers about the importance of maintaining the confidentiality and security of personal data.
7. Protection of personal data from loss, leakage, damage through adequate security controls.
8. Data efficiency through the implementation of backup, switch-over, and disaster recovery training efforts

In order to minimize the misuse of customer data, Bank Mandiri has launched Livin' Supper Apps with liveness detection and face recognition features so the customer can make financial transactions through mobile banking. With this feature, customer data is directly stored in the system without going through a

physical form. Livin' customers can change/ rectify their personal data, open savings accounts & apply credit cards, withdraw cash without a card, quick pick favorite transactions, instant e-money top up, and online shopping payments. Furthermore, Bank Mandiri ensure customer rights to rectification and control the personal data can be done in all branches or via call center 14000.

Bank Mandiri conducts periodic audits to perform assurance functions on all information security activities, including customer protection, data privacy, and fraud management, which are implemented in accordance with internal and regulatory regulations. The audit is divided into the following activities:

1. Internal Audit
   The internal audit process is carried out at least once in a year by a special IT Security Audit unit under the supervision of the IT Audit Unit (SKAI – Internal Audit Unit).
2. External Audit
   The external audit process is carried out at least once in two years by reputable international consultants (external independent parties). The external audit process is also carried out to comply with regulatory compliance aspects (BI) with the issuance of PBI No. 23/6/PBI/2021 concerning Payment Service Providers. In 2023, another external audit by reputable international consultants (external independent parties) with audit coverage covering customer protection, information security & data privacy, and fraud management.

Moreover, an assessment was also carried out by an independent external assessor, namely the State Cyber and Encryption Agency (BSSN) related to:

1. **Cyber Security Maturity (CSM)** assessment with maturity level 5 – **"Optimal"** (highest score). CSM assessment is an instrument from BSSN to assess the level of cybersecurity maturity of an organization, including the assessment of management maturity and protection of personal data privacy.
2. **Measurement of Incident Handling Maturity Level (TMPI)** with the result of maturity level 5 – **"Optimize"** (highest score). TMPI is a tool to map the level of organizational readiness in responding to and recovering cybersecurity incidents, including in detecting and responding if there is an incident of personal data leakage due to system security gaps.

The attendance of the Board of Commissioners and Directors directly at regular meetings of the Risk Monitoring Committee, Audit Committee, and Integrated Governance Committee demonstrates Bank Mandiri's forthrightness in monitoring information security. The committee meeting agenda includes: quarterly reporting on ESG initiatives on topics such as Privacy & Data Security, Bank Mandiri's multi-layer defense mechanism, and meeting Mandiri Group's security criteria.

The Security Awareness program is also carried out on a monthly basis to develop knowledge of information security in daily behavior, with the goal of making it the Bank's culture. Every year, Bank Mandiri provides security awareness training for all employees (at all levels in local and overseas offices) as well as third parties/contractors. Bank Mandiri also conducts regular security awareness campaign programs through various media, including a monthly newsletter, quarterly posters, quarterly podcasts, and a semester phishing drill. Data security protection, data confidentiality, latest cyber-attack trends, how to identify and avoid phishing, and online transaction security are some of the topics covered in the security awareness campaign.

Bank Mandiri also continues to increase customer security awareness by organizing educational programs through various official Bank channels, such as: website, social media (Instagram, Facebook, Twitter), and YouTube. Examples of education carried out through www.bankmandiri.co.id website with Digital Transaction Security links are educational content to maintain the confidentiality of personal data such as PIN, card validity period, 3 CVV numbers on the back of the card, card limit, User ID, password, and OTP.