Micmacs of Gesgapegiag

Information Management Policy and Procedures

Approved on September 13, 2022

Micmacs of Gesgapegiag

Information Management Policy and Procedures

TABLE OF CONTENTS

1. DEFINITIONS

“Arrears”	unpaid, overdue debt, or an unfulfilled obligation
“Assets”	anything of value owned by the Micmacs of Gesgapegiag “MOG”
“Asset Recognition Criteria”	criteria to be used to set the threshold for determining whether a capital asset must be included in the capital asset register
“Assign”	transfer of duties or functions from one person to another where the former person (the assignor) retains responsibility for ensuring the activities are carried out
“Authorization and Delegation Table”	a table approved by Council specifying the delegation and assignment authorities over decisions or activities related to the MOG financial administration
“Budget”	a plan or outline of expected money and spending over a specified period
“Capital Assets”	tangible capital assets (physical assets) such as buildings, land, and major equipment
“Capital Plan”	a consolidated plan or outline of expected money and spending of all capital projects to be undertaken in a fiscal year
“Capital Project”	the construction, rehabilitation or replacement of the MOG capital assets and any other major capital projects in which the MOG or its related entities are investors
“Capital Project Plan”	a project management plan to carry out a capital project that includes the budget
“Cash”	money, cheques, money orders, and equivalent forms of currency
“Cash Reserves”	money that a company keeps on-hand to meet short-term and emergency funding needs
“Classification”	process of categorizing records in an organized way
“Chairperson”	head of a meeting, department, committee, or board. The vice-chairperson acts as the head when the chairperson is not there

“Director General”	person who is responsible for leading the day-to-day administration or management of the MOG and who reports directly to Council
“Code of Conduct Declaration”	statement that Council, committee members, employees, and contractors must sign on an annual basis that states they understand and agree to the MOG code of conduct
“Committee”	group of people appointed by Council for advising Council or conducting decision-making activities assigned by Council until or unless they are suspended or disbanded by Council
“Conflict of Interest”	situation of personal gain at the expense of others
“Contract”	legally binding agreement between two parties
“Control”	policy, procedure, or process put in place to manage a MOG government’s administration
“Corrective Actions”	steps taken to deal with job-related behavior that does not meet agreed upon and communicated performance expectations
“Cost”	amount of money to be paid or spent to obtain something
“Council”	elected or appointed official representatives of the Micmacs of Gesgapegiag Chief, Councillors and the equivalent terminology used by Micmacs of Gesgapegiag
“Debt”	something that is owed or due, usually money
“Deficit”	shortage that occurs when an organization spends more money than it has on-hand over a period
“Delegation”	transfer of specific responsibilities from one person to another
“Director of Finance”	person responsible for the day-to-day management of the MOG finances
“Direct Supervisor”	employee responsible for managing and overseeing the work and development of other staff
“Eligibility Criteria”	requirements set by Council which must be met by an individual to be considered independent and eligible to be appointed to the Finance and Audit Committee

“Engagement Letter”	written document prepared by the auditor that serves as a contract to confirm the audit arrangements between the auditor and the MOG; it is required by Canadian Generally Accepted Auditing Standards
“Entity”	corporation, partnership, joint venture or unincorporated association or organization whose financial transactions are consolidated in the First Nation government’s financial statements in accordance with GAAP
“Expenditure”	amount of money spent by the MOG to buy goods or services
“Expenses”	amount of money spent on transportation, accommodation, meals, hospitality or incidentals, to be paid back (reimbursed)
“Financial Competency”	ability to read and understand the MOG financial statements
“Financial Reporting Risk”	possibility of a significant error in financial information often caused by weak internal controls or fraud
“Financial Statement”	formal record of all money and property of the MOG within a specific period
“Fiscal Year”	twelve-month period used for tax or accounting purposes
“Fraud”	wrongful or criminal act that involves lying or holding back information; this is usually done for personal or financial gain
“GAAP”	Canadian Generally Accepted Accounting Principles, the framework of accounting guidelines, rules and procedures
“HR Records”	records that contain information on an individual’s hiring, job duties, compensation, performance, and general employment history
“Indemnity”	security or protection against a loss or other financial commitment
“Independence”	eligibility criteria for finance and audit committee membership defined as an individual who does not have a direct or indirect relationship with the MOG government that could, in the opinion of Council, reasonably interfere with the individual’s judgment as a member of the finance and audit committee

	an individual with a role in the financial management of the MOG involving planning, organizing, directing or controlling of its financial activities – including budgeting, financial accounting, financial reporting, procurement and use of funds, does not meet the minimum independence requirements for finance and audit committee membership
“Information”	knowledge received and any documented material regardless of source or format
“Information Security”	the MOG protects information from unauthorized access, use, modification, or destruction
“Integrated Planning and Budgeting”	annual process of planning and budgeting activities across every level of the MOG that are linked, coordinated, and driven by the MOG vision and strategic objectives
“Internal Assessment”	review of an activity/process by an independent MOG staff member (i.e. an individual not responsible for or involved in the activity) to determine the effectiveness of that specific activity or process
“Investment”	an asset or item bought with the hope that it will gain value or provide income in the future
“Life-Cycle Plan”	plan of the MOG assets in terms of costs to buy, operate, upkeep and get rid of over a specified period
“Loan Guarantee”	promise to pay all or a part of the principal and/or interest on a debt obligation in the event of default by the borrower
“Local Revenues”	term used to describe property taxes under the *First Nations Fiscal Management Act*
“Materiality”	financial amount that the MOG government considers significant, typically large amounts; the materiality threshold is the minimum financial amount that the MOG government considers significant
“Misconduct or Wrongdoing”	breach of the MOG Financial Administration Law including conflict of interest provisions, code of conduct, Council-approved policies and administrative procedures
“MG”	Micmacs of Gesgapegiag

“Officer”	Director General, Director of Finance, Tax Administrator or any other employee of the MOG designated by the Council as an Officer
“Organizational Chart”	visual representation of the different positions at the MOG that clearly shows reporting relationships (who reports to who)
“Performance Improvement Plan”	plan developed by an employee’s direct supervisor, in consultation with the employee, to address the areas for improvement/development identified during the performance review process
“Personal Information”	information about a specific individual. In addition to common items such as an individual’s name, gender, physical characteristics, address, contact information, identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of an individual’s life
“Privacy Protection”	rules MOG puts in place to collect, create, use, share/disclose, retain, protect and dispose of the Personal Information that it needs for its administration
“Projection”	estimates for a future situation based on all the information available now
“Purchase Order”	document stating the wish of a buyer to purchase something from a seller that shows the exact details of the items the buyer wishes to buy
“Purchasing”	buying an asset or item. Also referred as “procurement” per the MOG’s Financial Management Board Standards
“Record”	information created, received, and maintained by the MOG for operational purposes or legal obligations. A record may be electronic, or hardcopy paper based
“Recordkeeping”	how an organization creates, obtains, and manages records
“Rehabilitation”	asset alteration, extension and renovation but does not include routine maintenance
“Remuneration”	salaries, wages, commissions, bonuses, fees, honoraria and dividends and any other monetary and non-monetary benefits

“Replacement”	substitution, in whole or in part, with another of the MOG capital assets
“Requisition”	purchase order used by the MOG when recording expenditures
“RFP”	Request for Proposal, competitive process followed by the MOG to enter a major service contract. RFPs lay out the MOG government’s needs and conditions and leave it up to the potential contractors to present a proposal that shows their experience, skills and ability to carry out the contract within time and cost specifications
“Risk”	possibility of a loss or other negative event that could threaten the achievement of MOG goals and objectives
“Sole Source”	contract entered by the MOG without a competitive process to purchase goods and/or services
“Special Committee”	committee formed for a specific purpose and is dissolved when that purpose has been achieved
“Special Purpose Report”	financial report on a specific activity
“Standing Committee”	committee that has an ongoing purpose
“Tax Administrator”	person responsible for managing the local revenues and local revenue account on a day-to-day basis, if the MOG is collecting local revenues
“Terms of Reference”	outline of the purpose and structure of a project, committee, meeting, or negotiation
“Travel Status”	pre-approved travel on official MOG business by an individual’s direct supervisor; Travel Status begins from the individual’s place of work (e.g. the MOG office) to the approved destination and ends once they return to their place of work
“Useful Life”	estimate of how long a capital asset is expected to be used by the MOG the life of a capital asset may extend beyond the Useful Life and the life of a capital asset, other than land, is fixed (limited)
“Value for Money”	best combination of price, quality, and benefits of a product or service
“Virtual Private Network”	VPN is a way to use public telecommunication infrastructure, such as the internet, to provide remote

offices or individual users with secure access to the MOG's virtual network

2. INFORMATION TECHNOLOGY

POLICY

Policy Statement

It is Council's policy to establish a process around the MOG information systems to support its operational requirements and have appropriate safeguards and monitoring processes in place.

Purpose

The purpose of this policy is to make sure that the MOG information is adequately protected and that the information system has integrity to maintain and support the strategic and operational requirements of the MOG.

Scope

This policy applies to all staff involved in the selection, implementation, operations, and ongoing maintenance of the MOG information systems.

Responsibilities

Council is responsible for:

- approving the information technology policy used by the MOG

The Director General is responsible for:

- ensuring that controls are in place over information technology, whether performed by an internal staff member or outsourced
- establishing and implementing documented procedures for information technology used by the MOG
- monitoring the performance of internal and/or external information technology professionals

ADMINISTRATIVE PROCEDURES

Procedures

2.1 Planning and Evaluation

The Director General, with input from information technology professional (internal and/or external), will make sure that information systems are developed that support the MOG strategic plan and operations.

When there are no individuals internally with the requisite technical skills to identify information technology requirements or evaluate options, the director general will seek advice from a qualified external individual or organization.

2.2 Outsourcing

Subject to the purchasing section of the finance policy, the Director General is responsible for the selection of contractors providing information technology services, the definition of services in their contracts, establishing service level agreements and the administration of the contracts.

Specific items which should be included in the procurement of information technology services and final contract with the chosen provider include:

- a requirement that the service provider submits regular reports of all work performed on the MOG information systems
- a requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information
- access by outsourced parties to MOG information is provided on a ‘need to know basis’ only
- time delays

2.3 Data Management

Subject to the Records Information Management section of this policy, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.

All sensitive, valuable, or critical data stored on the MOG information technology systems must be regularly backed-up; the MOG’s systems are backed up once every hour 7 days a week.

Backup drives must be stored in a secure location with access limited to the Director General and limited other staff as appropriate. Ideally, backup drives will be securely stored at an offsite location that is easily accessible to individuals with authorized access.

2.4 Access Management

All individuals requiring access to MOG information systems will have unique user identification. Shared user IDs or passwords is not permitted.

Requests for access to the MOG network, accounting system, or other access restricted information system must include a description of an employee’s role should include access in job descriptions and rationale for the level of access required. Signed approval must be obtained from the Director General.

User ID and password are required for access to the network and other critical programs/areas such as the accounting system.

Individuals will be given access privileges to the extent necessary to fulfill their individual job function and no more. Systems and applications should not be configured with unrestricted access to all data.

When an employee’s employment is terminated, their user IDs must be disabled immediately.

Support personnel must notify the user when attempting to take control of a workstation. All instances where specific software is loaded to remotely control a workstation must be removed

when the support function is completed. The use of the remote software must be in accordance with applicable agreements.

2.5 Information System Security

Security tools and techniques are implemented to enable restrictions on access to programs and data.

Security tools and techniques are administered to restrict access to programs and data.

Each computer resource must have an approved antivirus program installed. The following standards must be met:

- the antivirus program must not be disabled and must be configured to scan all programs and files upon execution and must have real time protection enabled
- antivirus files must be updated on the network regularly or whenever a new threat is identified

Network firewalls must be configured to support a ‘least-privilege’ approach to security, allowing only specific systems, services and protocols to communicate through the network perimeter. Logical and physical access to these systems must be limited strictly to those personnel with specific training and authorization to manage the device. Additionally, the following Firewall standards must be addressed:

- firewall and proxy servers must be securely installed
- detailed firewall logs must be maintained
- alerts must be raised if important services or processes crash

2.6 Change Management

All new data structure and modifications to data structure will be tested before implementation.

All computers, hardware, software and communication systems used for a production environment must employ a documented change control process. The change management process should include the following activities:

- data structure is consistent with the needs of the MOG
- description and rationale for the new network, hardware, communication and systems software change and how it is consistent with the needs of the MOG
- assessment of any risks involved with the change
- roll-back considerations
- implementation considerations
- description of required testing
- approval from the relevant Officer
- communication of changes to MOG staff as appropriate

2.7 Monitoring

Only approved and authorized programs will be implemented onto First Nation information management systems. The IT support will conduct periodic reviews of the workstations and the system to monitor compliance with this requirement.

A log of staff, their user IDs, and their access levels within MOG information systems will be maintained. On a periodic basis, the IT support will review the log to make sure users and the associated access rights are appropriate. Access rights that will be monitored include the following:

- user access management (i.e. the accounting system)
- third party access (i.e. outsourced information technology professionals)
- network access and file sharing
- remote and VPN access

Network system performance is monitored on a regular basis.

The firewalls must be monitored regularly.

References and Related Authorities

FMB's Financial Management System Standards

- Standard 20.0 – Risk Management

FMB's Financial Administration Law Standards

- Standard 19.0 – Risk Management

3. RECORD INFORMATION MANAGEMENT

POLICY

Policy Statement

It is Council's policy to establish a process around the creation, collection, organization, retention, and safeguarding of records for long term availability, understandability and usability.

Purpose

The purpose of the policy is to provide guidance on effective recordkeeping practices to create, manage and protect the integrity of the MOG records that support its decision-making, reporting, performance and accountability requirements.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the MOG and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all records created and acquired by the First Nation regardless of format (i.e., both electronic and paper records).

Responsibilities

Council is responsible for:

- approving the policy for records management

The Director of Communications and Policy is responsible for:

- establishing and implementing documented procedures for records management
- implementing appropriate recordkeeping practices
- ensure appropriate safeguards of the MOG records
- ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process
- ensuring that employees and contractors or volunteers performing services on behalf of the council are fully knowledgeable of their responsibilities as they relate to recordkeeping practices

The Directors of departments are responsible for:

- ensuring that employees and any contractors or volunteers performing services on behalf of the Council are fully knowledgeable of their responsibilities as they relate to recordkeeping practices

Employees, contractors and volunteers are responsible for:

- informing compliance with the established policy

- immediately reporting to their supervisor any potential breach related to compliance with the recordkeeping policy

ADMINISTRATIVE PROCEDURES

Procedures

3.1 Accountability

Each record will have a designated employee that makes sure the recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, or volunteers that are in custody of a record must make sure it is managed in accordance with this policy.

Permanent records such as policies and procedures will be reviewed and updated by the assigned employee on a regular basis.

Records under the safekeeping of a departing employee, contractor or volunteer must be formally transferred to another employee through a knowledge transfer process. This process should include information on the types of records to be transferred, how the records are organized, in which location the records are kept, and required safeguards.

All records produced, used, or received by the MOG remain the property of the MOG.

3.2 Creation and Collection

Key activities and decision-making processes of the MOG should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect the MOG from liability.

All information at its time of creation or collection should be assessed to determine if it supports Council's business purposes and/or legal obligations and enables decision-making. If determined to be a record, the management of the record should comply with the procedures outlined within this policy.

The record will contain information necessary to achieve the objectives for which each record is created and will be limited to only what is necessary to achieve those objectives.

Whenever possible, the record will contain information about one single function or activity to facilitate information classification, organization, retention and retrieval.

The MOG records will be legible, written in plain language and adapted to their specific audience.

Only one copy of each record should be created or collected. When creating or collecting a record, individuals should first check to see if the record is already in existence. In instances of multiple copies of the same record, copies should be securely disposed in accordance with the requirements of this policy.

3.3 Organization and Classification

A classification plan structure will be implemented based on the MOG functions and activities, with records stored in accordance with the activity and/or function that it supports.

Records should be subject to a consistent naming convention, with the name of the record including at minimum the title, version and date (t.v.d)

The title of the document should be short.

An official storage location will be identified and designated for each record. The number of storage locations should be limited and be consistent to support the format and type of record.

Records should be made accessible, shared and re-used to the greatest extent possible, subject to technological, legal policy and security restrictions.

3.4 Maintenance, Protection and Preservation

Records will be protected and stored in the appropriate storage location in a way that preserves their long-term availability, understandability and usability.

Backups will be taken of all electronic records on a regular basis and stored in a physical or digital location separate from the location of the original records.

Any records that are only in hardcopy paper-based format should be assessed to determine if they need to be scanned or if other physical security measures need to be taken (e.g. use of fire/water proof cabinets) to protect their long term availability.

Records that contain personal information or information of a confidential nature related to the Council, or a third party, such as the confidential financial information related to a business, should be labelled as **CONFIDENTIAL**.

Confidential records should be protected with appropriate safeguards to make sure only those with a need to know will have access to the records:

- for electronic records, confidential records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic storage location in which the record is stored
- for hardcopy paper-based records, confidential records will be always stored in secure filing cabinets unless being used, and transported in a secure manner if required to be offsite

3.5 Retention and Disposition

The records will be retained for the period specified in the records and information retention and disposition schedule, as outlined in Appendix A. They will be disposed of in a manner that prevents their reconstruction (for paper-based records) or recovery (for electronic records).

References and Related Authorities

The FMB’s Financial Management System Standards

- Standard 20.0 – Risk Management
- Standard 24.0 – Records and Information

The FMB's Financial Administration Law Standards

- Standard 24.0 – Records and Information

Attachments

1. Document Retention Periods

DOCUMENT RETENTION PERIODS

Record or information	Duration
General MOG governance records	
MOG laws, bylaws, legislative amendments, regulations, codes, directives, constitution, and membership resolutions	Permanent
Appointments and terms of appointments	Permanent
Agreements, funding arrangements, Council commitments	Permanent
Council meeting minutes, Council committee meeting minutes, annual reports, debenture records, membership records, public notices, records of incorporation, corporate seal, BCRs	Permanent
Legal files and papers	
Customer and supplier contracts and correspondence related to the terms of the contracts	7 years beyond life of contract
Contractual or other agreements (e.g., contribution, impact benefit, trust) between the MOG and others and correspondence related to the terms of the contracts	7 years beyond life of the contract
Papers relating to major litigation including those documents relating to internal financial misconduct i.e.: Criminal and civil litigation	5 years after expiration of the legal appeal period or as specified by legal counsel
Papers relating to minor litigation including those documents relating to internal financial misconduct Refer to delegation table	2 years after the expiration of the legal appeal period
Insurance policies including product or service liability, Council and Officers liability, general liability, and third-party liability, property and crime coverage	7 years after the policy has been superseded
Documents related to the purchase, sale or lease of property	Permanent
Documents related to equity investments or joint ventures	Permanent
Human Resources	
Personnel manuals and procedures	Permanent
Organization charts	Permanent
Where there is a pension plan (excluding RRSP plans): • original plan documents • records of pensionable employee service and eligibility • associated personal information including name, address, social insurance number, pay history, pension rate	7 years after the death of the employee or employee's spouse in the case of spousal eligibility

Letters of offer and individual contracts of employment	2 years after termination of the employee
Signed Code of Conduct obligations and signed Conflict of Interest declarations	2 years after termination of the employee
Attendance records	2 years after termination of the employee
Financial information such as payroll history including RRSP contributions, commission and bonus history	2 years after termination of the employee
Medical information	2 years after termination of the employee
Job descriptions	2 years beyond the period to which it applies
Performance assessments	2 years beyond the period to which it applies
Applications, resumes, and correspondence related to individuals not hired	2 years beyond the period to which it applies
Financial records	
Operations manuals, procedures, and internal control guidelines	Permanent
Signed annual financial statements and corresponding signed independent auditor reports	Permanent
Internal reports, including but not limited to: • reviews • special purpose reports • internal audit reports	10 years
Accounting documentation, including but not limited to: • general ledgers, general journals, financial records and supporting documentation • monthly and quarterly financial statements • monthly and quarterly management reports • month / quarter / year-end financial closing and reporting working papers • financial institution account statements and reconciliations • cancelled cheques and cash register tapes • invoices • annual budgets • multi-year financial plans	8 years

Asset management documentation, including but not limited to: • tangible capital asset register • reserve fund reports • life cycle planning • capital project budgeting • contract and tendering provisions	8 years beyond completion of the project or asset utilization
If applicable, property taxation related documentation, including but not limited to: • property tax working papers • tax roll • tax filings	8 years
Operational records	
Operations manuals, policies and procedures	Permanent
Original patents, trademarks, and copyrights	7 years after the expiration of the right
Customs documents	7 years
Annual physical inventories	Permanent
Safety committee minutes, inspection reports and related action reports	10 years
Backup drives	
Backup drives before being overwritten or deleted.	3 months

4. INFORMATION PRIVACY

POLICY

Policy

It is Council's policy to establish a process around ensuring the privacy of personal information provided to the MOG in compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or similar federal and provincial legislation.

Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within the MOG related to the collection, use, disclosure, retention, and safeguarding of personal information.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the MOG and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all personal information created and acquired by the MOG regardless of format (i.e., both electronic and hardcopy paper records).

Responsibilities

Council is responsible for:

- approving and complying with the policy for privacy and the management of personal information

The Director General is responsible for:

- establishing and implementing documented procedures for privacy and the management of personal information
- designating an employee to manage and oversee the MOG compliance with privacy requirements and this policy
- ensuring compliance with this policy

The designated employee who manages and oversees information privacy function is responsible for:

- developing and maintaining standards, policies and procedures that support the objectives of the MOG privacy program
- making sure that all the activities of the MOG are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the employee will:

  - provide training and awareness on privacy protection
  - ensuring that community members are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the personal information which is kept about them by the MOG
  - acting as an expert resource on privacy matters
  - conducting periodic reviews of the MOG activities that involve the collection, use, disclosure, retention, and safeguarding of personal information
- investigating all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of personal information and reporting the results to the appropriate supervisor and, where warranted, to Council
- recommending changes to policies, procedures and practices in response to the issues raised in the complaints
- responding in writing to the requests for access to, and correction of personal information submitted by employees and community members within 10 days from the date of the receipt

Employees, contractors and volunteers are responsible for:

- complying with the established policy
- immediately reporting to their direct supervisor any privacy breaches

ADMINISTRATIVE PROCEDURES

Procedures

4.1 Accountability

The Director General will designate an employee to make sure the principles outlined in this policy are implemented.

4.2 Identifying Purpose

The purposes for the collection of personal information should be communicated to individuals at or before the time of collection. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected.

4.3 Consent

With limited exceptions, the MOG must obtain consent, verbal or written, from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be used and disclosed.

Consent must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent must not be obtained through deception.

Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances, such as legal or security reasons which may make it impossible or impractical to seek consent.

If personal information is intended to be used or disclosed for a new purpose not identified during the original collection, and not related to the original purpose of the collection, the consent of the individual must be obtained.

Individuals can give consent in many ways. For example:

- a form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information; by completing and signing the form, the individual is giving consent to the collection and the specified uses
- consent may be given orally
- consent may be given through electronic means

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

4.4 Limiting Collection

The MOG cannot collect personal information unethically. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

4.5 Limiting Use, Disclosure and Retention

Personal information will only be used or disclosed for the purpose for which it was collected, specifically:

- consistent with the original collection of the personal information
- when consent of the individual is obtained
- for complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information

Personal information that has been used to decide about an individual must be retained long enough (minimum of 5 years) to allow the individual access to the information after the decision has been made.

Identifiable personal information must only be used and disclosed if required.

Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with the MOG retention and disposition schedule.

4.6 Accuracy

The MOG will take all reasonable steps to make sure that personal information that is used to decide on an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.7 Safeguards

Personal information should be protected with appropriate safeguards to make sure only those with a need to know will have access to the records:

- for electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic storage location in which the record is stored
- for hardcopy paper-based records, containing personal information, the records should be always stored in secure filing cabinets unless being used, and transported in a secure manner if required to be taken offsite

The MOG must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.

Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

4.8 Openness

The MOG must be open about its policies and practices with respect to the management of personal information. Individuals will be able to easily acquire information about its policies and practices. This information must be made available in a form that is generally understandable.

The information made available should include:

- the name or title, and the address, of the designated employee overseeing information privacy, who is accountable for the MOG policies and practices, and to whom complaints or inquiries can be forwarded
- the means of gaining access to personal information held by the MOG
- a description of the type of personal information held by MOG

4.9 Individual Access

When requested, an individual must be informed if the MOG holds personal information about the individual and provided an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

The identity of an individual will be authenticated before discussing their personal information with them.

When requested, the MOG must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable.

Individuals who are given access to their personal information may:

- request correction of the personal information where the individual believes there is an error or omission therein
- require that a notation be attached to the information reflecting any correction requested but not made
- require that any person or body to whom that information has been disclosed for use for a decision-making process, within a reasonable time that a correction or notation is requested, be notified of the correction or notation

In certain situations, the MOG may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that:

- contains references to other individuals
- cannot be disclosed for legal, security, or commercial proprietary reasons
- is subject to solicitor-client or litigation privilege

4.10 Challenging Compliance

The MOG will make sure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

If a complaint is found to be justified, the MOG will take appropriate measures, including, if necessary, amending its policies and practices.

References and Related Authorities

FMB's Financial Management System Standards

- Standard 12.0 – MOG Managers and Employees
- Standard 20.0 – Risk Management
- Standard 24.0 – Records and Information

FMB's Financial Administration Law Standards

- Standard 24.0 – Records and Information