**INFORMATION SECURITY POLICY**



**LEKET ISRAEL ASSOCIATION**

1 Background 3

2 Purposes 3

3 Application and Validity 4

4 Definitions 5

5 Applicable Documents 5

6 Responsibility for Information Security 5

7 Method – Security Circles 10

8 Measures 12

9 Enforcement 18

10 Updates and Changes in the Policy 18

11 History of Updates 18

**1 Background**

1. Leket Israel is an association which constitutes a nonprofit organization operating a national food bank and food rescue network by means of donors, volunteers and welfare organizations for rescuing and distributing food surpluses to those in need of it.
2. Leket Israel operates in internal and external environments that include entities which affect the success of the association and the continuity of its affairs. These effects are economic, technological, political, legal/regulatory, social or environmental.
3. The internal entities that affect the association are: its conduct as a nonprofit organization, a variety of procedures, cultural and human resources, including employees and volunteers of various types and information systems in a public cloud environment. Among the external entities that affect the association are donors, suppliers, regulators (the Privacy Protection Authority, the Registrar of Societies), variable market conditions and even state security threats, as Leket is an Israeli association that includes the word “Israel” in its name, together with the slogan “National Food Bank”.
4. The association’s assets include information, systems, procedures and key personnel. The purpose of information security in the association is to protect the association’s assets against internal and external threats. These threats are liable to be realized as the result of human error or a technological malfunction, but also intentionally and maliciously.
5. Harm to the association’s assets is liable to cause damage to the privacy of the people (those in need, employees, volunteers and donors to the association), as well as operational, technological and financial damages and harm to the reputation and image of the association in Israel and abroad.

**2 Purposes**

1. The principles of information security are based on a risk management system that identifies, controls, minimizes or prevents the security risks that are liable to affect the information, the systems and/or the procedures connected to them. The defense will be done with regard to parameters of confidentiality, integrity and availability of all those assets held and owned by the association.
2. The purposes of the Leket information security policy as defined by the administration of the association are detailed below and are used as guidelines for the implementation of information security in the association:
	1. Determining the principles guiding the implementation of the information security and providing a framework for the central tools and procedures on the subjects of information security, while creating an infrastructure for comprehensive procedures in the various fields.
	2. Reducing the likelihood of a significant information security incident occurring in the association.
	3. Reducing the damage that is expected to be caused as the result of the occurrence of a significant information security incident.
	4. Improving the resilience, durability and ability of the association to recover quickly from cyber incidents.
	5. Maintaining the confidentiality, availability and integrity of the business information of the association, the processes and information systems as well as the private and sensitive information of employees, donors, suppliers and supporters of the association which is processed and stored in the association’s systems.
	6. Determining guiding principles for the protection of private information located in the databases of the association pursuant to privacy laws.
	7. Complying with the requirements of the laws applying to the association and the contractual engagements to which it is subject in an optimal manner.
	8. Raising awareness of information security among the managers and employees and raising the professional competence of those occupied in the field of information security in the association.

**3 Application and Validity**

1. This policy applies to all the employees of the association, all the organizational procedures, all the information systems, infrastructure and the cloud, all the networks possessed and managed by the association and all the installations connected with them and owned by or in the possession of the association.
2. Volunteers, suppliers and external consultants (whether employed at the association’s sites or providing services remotely), are bound by the information security policy and procedures of the association in connection with the provision of the services or supply of the products to the association and pursuant to the contract with them or with the organizations via which they provide their services.
3. The administration of the association (hereinafter: “**Administration**”) views all the managers and employees as full partners in the effort to protect the confidentiality, integrity as well as the availablility of the information, the systems and the procedures in the association and expects cooperation in the implementation of the policy and the rules derived from it.
4. This policy is valid from the date of its approval by the Administration.

**4 Definitions**

1. **Privacy Laws** – The Privacy Protection Law and Privacy Protection Regulations (Information Security, 5777-2017 and all the guidelines of the Privacy Protection Authority and the rulings and guidelines of the courts and authorities in Israel relevant to Leket in the area of information security, cyber and privacy protection.
2. **Information** – all the data connected with the activity of Leket, including data that exists on computerized storage media, magnetic or electronic media and on physical platforms.
3. **Private Information** – information relating to a private person or an authorized dealer, including one or more of the following: data on the personality of the person, his personal status, personal privacy, state of health, economic condition, professional training, opinions and belief.
4. **Sensitive Information** – Business information the revealing of which to unauthorized entities is liable to cause harm to privacy, significant business damage to Leket or liable to be a breach of law or regulations, or private information of the following types only: data on the personality of the person, his personal privacy, state of health, economic condition, opinions and belief.
5. **Leket, or the Association** – From Table to Table Leket Israel (Reg. Assoc.).
6. **Steering Committee for Information Security** – as defined in Clause 6.1 below.

**5 Applicable Documents**

1. Privacy Protection Law, 5741-1981.
2. Privacy Protection Regulations (Information Security), 5777-2017.

**6 Responsibility for Information Security**

The organizational entities and frameworks having the responsibility to implement the information in the association:

1. **Steering Committee for Information Security**
	1. The purpose of the steering committee for information security is to determine the strategy for managing information security in the Association and to control its execution.
	2. Composition of the steering committee
		1. CEO of the association – chairman of the committee
		2. Information security manager – secretary of the committee, responsible, inter alia, for the summoning of the committee, the keeping of minutes of the committee meetings and the agenda
		3. Information system manager
		4. CFO
		5. Legal consultant
		6. Human resources manager
		7. Managers of additional business units will be summoned as needed
	3. Functions of the steering committee

6.1.3.1 Defining the policy and procedures of the Association in the areas connected with information security and protection of privacy and monitoring the implementation.

6.1.3.2 Defining the indicators for determining the risk level as well as indicators for examining the constant improvement on the subject of information security and privacy protection.

6.1.3.3 The committee will approve the risk assessment and the work plans and resources for handling gaps found in reviews and surveys of information security and privacy protection and will carry out control over their execution.

6.1.3.4 The committee will convene once every six (6) months and immediately following each significant incient that is liable to influence the area of information security (such as: changes in the information systems, a severe information security event, etc.) and will keep a protocol of its meetings.

1. **Information Security Manager**

The information security manager is subject to the IT manager and responsible for acting in accordance with what is detailed below, in order to minimize the risks of a significant cyber or information security event materializing which may materially affect the functioning of the association. For this purpose:

* 1. He will oversee and supervise the area of information security and privacy protection in the association.
	2. He will advise the Administration on all the subjects connected with the management of cyber protection and the protection of privacy.
	3. He will assist the Administration in the forming and implementing of a policy on information security, cyber and privacy protection and will guide it in the areas of corporate governance, risk management and regulatory compliance.
	4. He will formulate a methodology for managing cyber and information security risks by creating and updating policies and procedures and providing guidelines in accordance with the laws and regulations applicable to the association in the fields of information, privacy and cyber security.
	5. He will lead in the definition and management of cyber risks in the association and will work together with the relevant (technological and business) entities in the association in the analysis and evaluation of the levels of inherent risk in the activity, the required controls and, accordingly, the levels of residual risk and exposure to cyber threats.
	6. He will promote and manage the creation, maintenance and improvement of information security procedures while implementing cyber and privacy protection controls in the information systems and processes of the association.
	7. He will increase organizational awareness of cyber and privacy protection threats, the training of relevant employees, volunteers and suppliers of the association regarding the ways of dealing with them, including legal and regulatory requirements as well as the policy and procedure documents of the association in these areas.
	8. He will perform audits and supervision of the operations of the association and its suppliers in the areas of information security, cyber and privacy protection and the implementation of the provisions of law and regulation applicable to the association, with the aim of increasing the level of information security and privacy protection in the association.
	9. He will lead the formulation of scenarios demonstrating the realization of cyber and privacy protection risks in the association and will lead exercises for organizational dealing with attacks of various types by parties both outside and within the association in cyber space as well as in physical space.
	10. He will coordinate and link the association and external parties (suppliers, regulators, volunteers, donors and others) regarding cyber protection issues.
	11. He will develop relevant indicators, prepare reports and report periodically to the Administration in his areas of activity.
	12. He is responsible for the overall management, investigation and control of cyber and privacy protection incidents in the association.
	13. He will test and integrate new information security and privacy protection technologies in the association.
1. **IT Manager**
	1. The IT manager has the overall responsibility for information security and information systems at Leket and will act as liaison between the information security manager and the senior Administration of Leket. In the event of an information security incident, he will be included and will manage the technological protection activity.
	2. The IT manager is responsible for the proper, professional operation of the Leket information systems and information security as well as the implementation of information security policies, procedures and controls in these systems.
	3. The IT manager will assist in everything connected with communication and contractual engagements with the computing suppliers and supply chain of Leket. More generally, he will assist the information security manager in assessing and managing supply chain risks and will act as liaison with suppliers in periodic and dedicated assessments of information privacy and security risks and in contractual engagements with them.
	4. In the event of a conflict of interest between the duties of the IT manager and his responsibility in matters of information and cyber security and/or in the event of a dispute between the IT manager and the information security manager, it is the responsibility of the information security manager to bring the issue to the CEO of Leket for a decision.
2. **The Administration of the Association**
	1. The managers of the association will supervise the implementation of information security policies and procedures by their employees and will support information security and privacy protection activities, each in his or her own professional field.
	2. The method and those responsible for managing the databases in the association, pursuant to the requirements of privacy laws, will be determined in the database management procedure.
	3. The legal advisor (hereinafter “**Legal Advisor**”) will provide dedicated and ongoing legal advice for all the legal aspects of these operations to be carried out by the employees and suppliers of the association on its behalf. Among other things, the Legal Advisor, in cooperation with the information security manager, the human resources manager of the association and other administrative individuals that they deem appropriate, will determine the privacy protection policy of the association and supervise its implementation pursuant to the laws applicable to Leket, each in his or her own professional field.
	4. The human resources manager (hereinafter “**HR Manager**”) will assist the information security manager regarding the conducting of training and awareness activities for the employees and volunteers of the association and any additional assistance required.
	5. The purchasing manager (hereinafter “**Purchasing Manager**”) will assist in all matters relating to communication and contractual engagements with suppliers and the supply chain of Leket other than computing suppliers. In general, she will assist the information security manager in assessing and managing supply chain risks and will act as liaison with the suppliers in periodic and designated information and privacy security risk assessments in contractual engagements with them.
	6. The deputy manager of operations and logistics will be responsible for the physical security at the logistics center.
	7. The CFO will be responsible for the physical security at the offices of the association and all other premises where Leket operates.
3. **Employees of the Association**
	1. All the relevant employees and third parties of the association are responsible for maintaining the security and confidentiality of the information they use and to which they have been given access.
	2. The employees of the association are responsible for reporting any suspicion of information security incidents to the information security manager or to the IT manager.
	3. The employees of the association must be aware of the risks of exposing information and unauthorized use of information and must act in accordance with the procedures of the association and its guidelines as given from time to time in order to minimize the risks of information leaks to unauthorized persons or other harm to information security and privacy protection.
	4. Suppliers, consultants and other third parties providing services and goods to the association are responsible for their employees, subcontractors and anyone acting on their behalf.

**7 Method – Security Circles**

Information security, cyber and privacy protection in Leket will be carried out by all the entities involved, by means of the security circles detailed below (for each of them, detailed procedures have been defined):

1. **Physical security**: physical security constitutes the first circle in information security.
	1. The communications room will be protected from unauthorized entities; control and access documentation will be executed. Entry will be permitted only to those authorized for this for the purposes of support and maintenance of the communications equipment.
	2. The communications room will contain only communications equipment, and no other equipment.
	3. The offices and logistics center of the association are monitored by means of CCTV to provide a warning of unauthorized access and to document any suspicious activity.
	4. Sensitive information found in documents and physical folders will be kept in locked cabinets or rooms at the end of each work day.
	5. Critical and sensitive information will be protected physically from unauthorized access, damage and interference, failures in power supply or other disturbances caused by unauthorized access or failures in support services.
2. **Logical security and cloud resources**: the principal computerized resources of Leket are located in a cloud network and cloud services of various kinds.
	1. Leket will take measures to protect the security of the information stored and processed by various cloud services (SaaS, PaaS, IaaS) and will implement security measures needed to protect the cloud resources, the scope of the security and the internal networks.
	2. The information security manager will outline the level of logical security required for the various components of the computer and communication systems of the association, subject to the laws and regulations to which the association is subject.
	3. In order to minimize information security risks from the Internet, a strict policy will be implemented with regard to the isolation of the Internet environment from the systems of the association, in surfing from the means provided, secured and monitored by the association.
	4. The contractual agreements with the cloud providers will include an information security annex in which the joint responsibility model and security requirements will be summarized, which include, inter alia, encryption of the information in motion and at rest, secure identity management, monitoring, backups, implementation of access controls and security measures based on the classification of the information, the ability to respond to events and business continuity.
	5. Leket regularly (and at least annually) will assess the security of the cloud providers and the cloud environments in relation to the risks to Leket and the information stored or processed in the appropriate cloud service. If the need arises, it will strive to amend the contractual conditions with the cloud provider in order to provide a better response to a change in risk.
	6. Use of cloud resources will be managed while complying with all the relevant laws, regulations and standards in industries connected with the storage and processing of private information in the cloud.
3. **Supply chain security**: information security aspects will be defined in communications and work with external suppliers and service providers throughout the supply chain, and they will be integrated into contractual engagements and day-to-day work with the suppliers. This will include:
	1. Suppliers will be classified according to their level of criticality to Leket and according to the sensitivity of the information and the depth of access they will receive to the Leket information and systems, in accordance with the method established in the regulation.
	2. In every contractual agreement with a supplier or service provider, information security and cyber and privacy protection principles will be defined in a dedicated appendix, according to the sensitivity of the information and systems to which the supplier and those on its behalf will have access.
	3. Periodic risk surveys and annual information and cyber security protection and privacy risk assessments will be conducted in order to examine the risks arising from each relevant provider, in accordance with a systematic method that complies with the guidelines of the regulations.

**8 Measures**

The association will implement the measures and act in the ways detailed below in its manner of implementing the policy in the areas of information security and cyber and privacy protection:

1. **Corporate governance**: the association will create a clear corporate governance process led by the senior Administration, for the promotion, budgeting and supervision of the information security, cyber and privacy protection framework.
2. **Information security procedures**: the information and cyber security manager will be responsible for writing and maintaining the policy documents and information security procedures. These policies and procedures will establish standards and guidelines for the implementation and ongoing operation of the security and control measures for the information and ICT resources of the association, including work processes and guidelines for employees. The policy documents are to be approved by management.
3. **Risk management**: the association will operate according to an orderly and monitored methodology for managing and reducing the risks to which it is exposed. The risk management process will include, inter alia, the following:
	1. Defining the major risks of the association.
	2. Defining the risk appetite of the organization.
	3. Mapping, analysis and recording of threat scenarios, threats and exposures.
	4. Mapping, analysis and recording of risks in an organized risk registry, with reference to the relevant laws and regulations on the one hand and to the IT, organizational procedures and human factors relevant to the above-mentioned risks on the other.
	5. Preparation and implementation of a work plan based on the risk management process.
	6. Effective mapping and analysis of controls in the association, drawing of conclusions and their orderly assimilation in the risk management process.
	7. Updating and refreshing the process in a fixed, orderly manner.
4. Leket will carry out risk surveys and penetration tests at least once every 18 months for all its relevant IT systems, cloud and communication resources of the association, the organizational applications and the organizational processes.
5. An internal or external audit will take place at least once every 24 months, by a person with appropriate training for an audit on the subject of information security, to verify compliance with the provisions of privacy laws.
6. **Annual and multi-year work plan**: as part of the annual and multi-year planning, the association will also integrate a work plan to improve the robustness of information security, cyber and privacy protection. The plan will be based on gaps found during the year and improvements required due to organizational changes, technological developments and new risks. The plan will be compiled by the information security manager and will be submitted for the approval of the information security steering committee. After its approval, the plan will be implemented and audited according to the procedures of the organization.
7. **Management and classification of information and assets**:
	1. Leket will establish a procedure for managing information assets which will define parameters for determining the types of assets that will be mapped and managed, the criticality of the assets, ownership, classification, handling and destruction, as well as periodic review and updating.
	2. Leket will create and update a diagram describing the architecture of the active networks in Leket (local, cloud, WiFi, etc.), connections between the networks and interfaces to email and other SaaS and PaaS resources, a description of the segmentation within each network, the directions of information flow between the parts of the network and the various systems, the information systems and physical components of the networks, the information security systems installed in each network, the links between them, etc. (a physical and logical diagram of each network and all its components).
8. **Human resource security**:
	1. A procedure for the secure management of human resources, including volunteers of various types, will be defined and implemented in the organization; it will include guidelines throughout the life cycle of the worker, including hiring, transitioning between roles and termination of employment, in order, inter alia, to prevent abuse of access rights and privileges.
	2. Verification checks (such as a background check) will be performed for all employees, especially those employed in sensitive positions, as well as relevant outsourced and other employees; these will be determined by the information security manager in consultation with the deputy director of human resources and other relevant managers.
9. **Management of databases**: a procedure will be defined for the management of the private databases of Leket in accordance with privacy laws and accepted rules of information security. Database managers will be chosen; the roles and responsibilities of the database managers and other officials in Leket will be defined in connection with the secure management of the databases.
10. **Permissions and access control**:
	1. A policy will be defined and implemented for granting permissions, user identification and control of access to systems and information in Leket according to role and professional need. Rules and principles will be defined for providing access to information and information systems and throughout the life of the user in the organization, and the principles of “need to know” and “least privilege” will be applied for the purpose of granting permissions and managing changes in access permissions.
	2. Each of the database managers of Leket will be responsible for the permissions given for the database under his or her responsibility.
	3. An automatic documentation and control mechanism will be managed for every attempt to connect to the network resources and systems of the association and every activity therein. External access will be permitted only through the security systems of the association.
	4. A periodic review of users and permissions will be conducted in the systems of the association, as well as the closing of inactive users, reducing and applying access permissions according to the “need to know” principle.
	5. Privileged (strong) permissions and users will be managed more strictly, while implementing stricter-than-usual information security measures.
11. **Handling of information security incidents:**
	1. Leket will define a procedure for managing information security incidents in which principles and processes will be established for identifying, reporting and managing the incidents; incident handling teams (a management team and an operational team), escalation processes, management involvement, classification of events, notifications and involvement of parties external to the association, documentation and investigation capabilities and the drawing of conclusions will also be defined.
	2. The IT manager is responsible for managing and including the technological protection activity in the event of an information security incident and together with the information security manager will assist the Administration of the association in making decisions and managing information security incidents according to their severity, as detailed in the information security incident procedure.
	3. All relevant employees, outsourcing providers, volunteers and third parties are required to report to the IT manager, and he will update and consult with the information security manager with regard to security incidents and vulnerabilities of which they are aware.
	4. Information security incidents will be investigated, and the conclusions of the investigation will be discussed in the information security steering committee. Serious incidents will be brought to senior management for discussion. For the needs of the investigation, Leket will establish and implement work rules for identifying, collecting and keeping evidence related to information security incidents. The knowledge gained following information security events will be used to strengthen and improve information security controls and, if necessary, to update this policy and the information security and privacy protection procedures.
12. **Awareness and training:**
	1. Leket will develop and implement a comprehensive, measurable information security and privacy protection awareness program and will hold training sessions for all relevant employees and third parties according to their role, the classification of the information and assets they are exposed to and their access privileges.
	2. The program will include, inter alia, training sessions and exercises for new employees and volunteers following their absorption, during significant changes and events and during an annual refresher. The processes will be documented and checked in order to improve and optimize the activity and awareness.
13. **Remote work**: information security rules and guidelines will be defined and implemented for access, by association employees and necessary entities, to the resources and information assets of Leket during remote work.
14. **Security of mobile computing devices**: the principles, method, work processes and measures will be defined and implemented in order to enable the secure use of laptops, cell phones, terminals and other mobile devices.
15. **Management of removable media**: processes will be defined for the management, handling, secure transfer and disposal of portable storage devices and removable media in order to prevent information leaks, information theft, unauthorized access to information and potential damage to information assets through malicious software.
16. **Protection of endpoints and servers**:
	1. Leket will define and implement a hardening policy for workstations and servers that provides a response to the information security requirements of the organization.
	2. Leket will increase network protection capabilities by implementing advanced, proactive tools and work processes in order to provide better protection against new and unknown information security policy threats (zero day risks) and, if possible, will strive to implement a zero trust policy both within and outside the Leket networks and information assets.
17. **Monitoring and control**: Leket will establish a documentation policy in accordance with the regulatory requirements applicable to the association and its business/operational needs regarding the documented information, duration, and manner of saving the logs in the various systems and to be applied to the various systems.
18. **Separation of networks**:
	1. The ICT infrastructures of the association (IT, local and/or cloud) will be designed using the approach of separating networks in order to reduce as much as possible the risk of “contagion” between different resources by damages and risks from a cyber attack. The separation will be based on the potential for damage and harm to the aims of the association, while minimizing the operational damage to employees in their day-to-day activities.
	2. Leket will plan and act to carry out network segmentation that reflects the access permissions – separation between an external network and an internal network, servers, end users, equipment and cameras, using FW (firewall) rules and a transfer to managed network switches for implementation. In addition, separation will be implemented by means of an FW within the cloud resources and between them and other resources in Leket networks in accordance with the principles of “need to know” and “least privilege”.
19. **Secure development**: aspects of information security and privacy will be defined and implemented by default as early as the planning stage and throughout the development processes of systems and information assets in Leket as well as by relevant development service providers.
20. **Change management**: a change management process will be defined, documented and implemented to ensure that changes in systems, processes and information assets are controlled and implemented by relevant employees and third parties.
21. **Backups**: backup requirements will be defined for each relevant system and the types of information related to it, according to the organizational processes, criticality and classification of the systems, information, and processes. The backup requirements will be incorporated into the relevant systems and contracts with suppliers that support the backup and recovery processes.
22. **Business continuity**:
	1. Leket will determine a disaster recovery plan to reduce the impact on the organization and enable faster recovery in various disaster cases, which include loss of information or information assets, lack of access to critical information assets, etc.
	2. Leket will identify the critical functions and processes that depend on and are supported by the information and information assets of the organization and perform a business impact analysis (BIA) of the consequences of disasters, substantial business disruptions, security failures, loss of service or information, unavailability of information. Critical business processes will be included in the disaster recovery plan (DRP), and recovery parameters will be determined for them in terms of schedule and amount of information (reovery point objective – RPO – and recovery time objective – RTO) in accordance with the business requirements of the association.
	3. The resilience of Leket will be planned, implemented, maintained, practiced and tested, based on business continuity goals and business continuity requirements determined by the information security steering committee.
	4. Leket will determine controls that, as far as possible, will permit maintaining an adequate level of information security even during a substantial disruption as mentioned above.

**9 Enforcement**

1. The Leket managers will be responsible for enforcing this policy and information security procedures with their employees. Disciplinary measures will be taken against an employee who has acted contrary to the procedures of the organization relating to information security; among other things, they will take into account the severity of the violation and its consequences.
2. Each disciplinary offense will be recorded in the personal file of the employee and will be taken into account for performance evaluation purposes.

**10 Updates and Changes in Policy**

1. The information security manager will review and, if necessary, update the information security policy and procedures every year as well as as a result of risk assessment processes, organizational changes, changes in legal or regulatory requirements, changes in the business environment, changes in the IT infrastructure, information security events and external and internal influencing factors.

**11 History of Updates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Person Updating**  | **Details** | **Person Approving**  |
| 1.0 | 22/5/2023 | Inbar Ben Zion Regerman, Information Security Manager | Creation of policy | IT ManagerLegal Consultant \_\_\_\_\_\_CEO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |  |