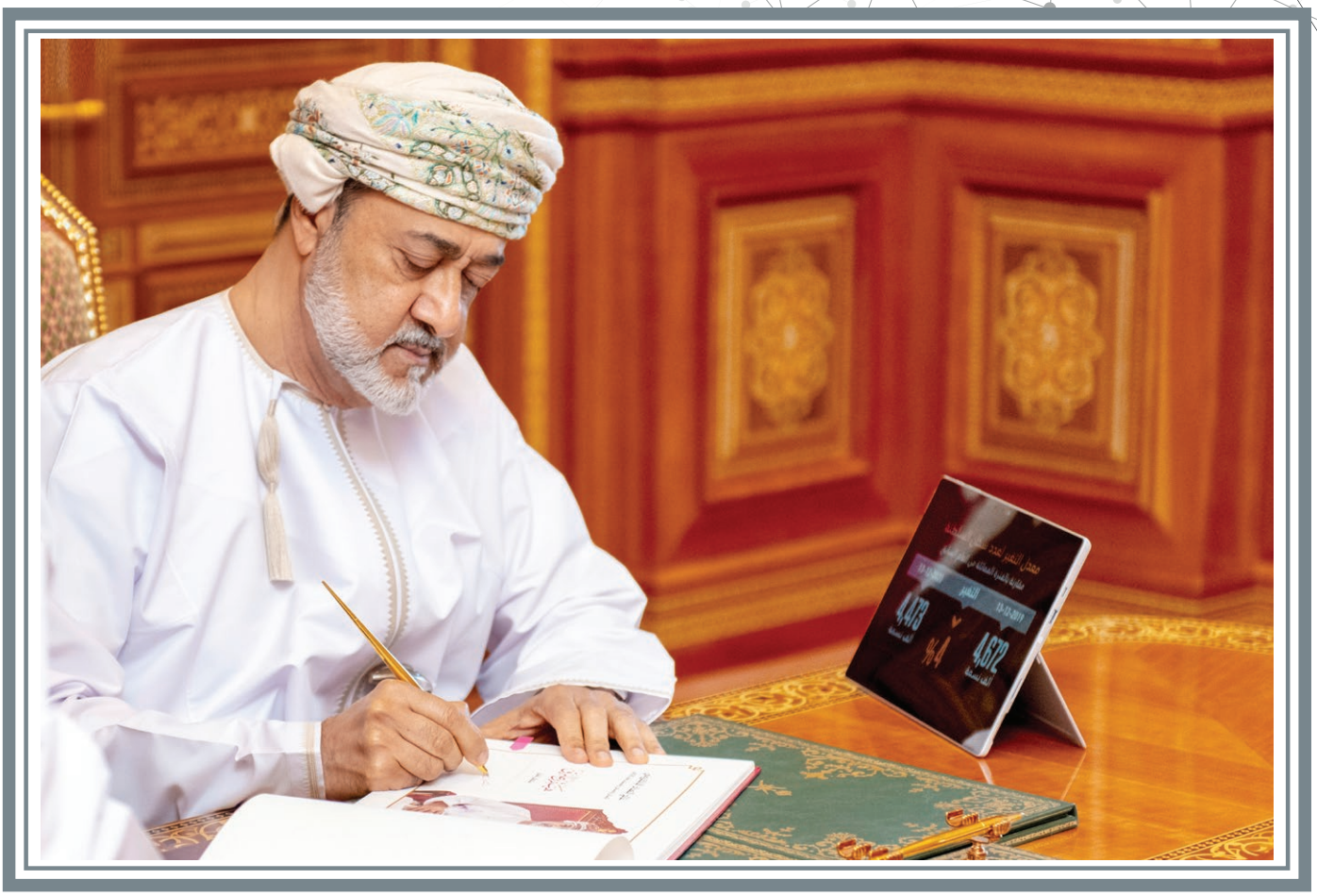
رؤية عُمان 2040
تعداد 2020
التعداد الإلكتروني للسكان والمساكن والمنشآت
Electronic Census of Population, Housings and Establishments
NATIONAL CENTRE FOR STATISTICS & INFORMATION
Enhancing Knowledge
SULTANATE OF OMAN

Information Security Management for the E-Census

for Population, Residences & Establishments

2020

E-Census Documents
Series 2020
03



His Majesty Sultan Haitham Bin Tarik

- may Allah protect him-

endorses E-Census 2020 results of Population, Residences and Establishments as of 12 December 2020. His Majesty the Sultan expressed his satisfaction with the outcome of this major project which was implemented as scheduled. His Majesty the Sultan underscored the significance of data and indicators provided by the Census in enhancing Oman Vision 2040, as well as the Census's important implications to developmental planning in all sectors of the Sultanate.

14 December 2020

Table of Contents

Introduction

The electronic census 2020 relied in its methodology on electronic administrative records in the country, through which data on population, residences and establishments are collected. This information and data are deemed as confidential and it is banned to be passed around or produced except in an aggregate form and for statistical purposes only in accordance with the Statistics Law issued by Royal Decree No. 29/2001.

In order to protect this data, a document has been prepared in the electronic census project that illustrates the mechanism of information security management and the mechanism of collecting, using and saving information collected from government and private institutions and other entities about individuals, residences and establishments, while ensuring the availability of this information to the persons authorized in dealing with this data and information.

This document has been prepared taking into account its compatibility with the Statistical Law issued by Royal Decree (29/2001), the Law for Classifying State Documents and Organizing Protected Places, issued by Royal Decree No. 118/2011, and the Electronic Transactions Law issued by Royal Decree No. (69/2008) and it follows the good practice, the Law on Combating Information Technology Crimes issued by Royal Decree 12/2011 and Royal Decree No. (15/2015) for conducting the electronic census of population, residences and establishments for the year 2020 and the policy of Information Security for Information Technology Authority.

This document further deals with the information security policy, which defines the policy set by the project management and the administrative bases for information security in the E-Census 2020 project, as well as the acceptable use policy, which defines the acceptable practices related to the use of information resources in the E-Census 2020 project. It includes but not limited to, data, computing equipment, software, network services, e-mail, Internet / intranet and storage media. This policy further contains the minimum that every employee must know in addition to the security awareness policy that informs employees that information security is everyone's responsibility and that everyone is required to learn about information security and attend events / trainings / workshops related to information security.

1 | Information Security Policy:

1.1. The Purpose

The purpose of this policy is:

- Managing of guidance, support and compliance with the information security policy in the electronic census project 2020.
- Inform all E-Census 2020 project contract employees, project teams in government and private institutions, and people associated with work related to the project about their responsibilities and obligations with regard to information security.
- Ensuring the availability of sufficient resources to implement an effective information security management system.
- Identify and reduce risks arising from any security flaw that the project may be exposed to.
- Ensuring the continuity of work in the project without interruption resulting from a defect in information security.

1.2 Scope

This policy investigates all forms of information and comprises data stored on computers and servers, transmitted over networks, printed or written on paper, faxed, stored on tape or discs, transmitted in a conversation or over the phone.

Facilities: The Head Office of the Electronic Census Project, all buildings and units within the scope of the project, all employees, contractors and teams of the project in government and private institutions, and all suppliers, companies and persons related with works with the project.

Data: preliminary and processed data includes:

- Electronic data files: includes all electronic files regardless of their storage media.
- Paper documents: includes all documents and paper documents.

Software: includes all locally developed software and software obtained from external sources.

- Application software, operating system software and all associated utilities and support software.

- Application-enabled programs including database management, middleware, telecommunications, and network software.

Employees: All employees, contractors and project teams in government and private institutions, all suppliers, companies and people working on the project.

1.3. Policy

The E-Census 2020 project will implement all possible and relevant measures to achieve the following objectives: -

Availability: Establishing controls and procedures to ensure that information is accessible to authorized persons and to ensure recovery in the event of a malfunction.

Integrity: Establishing controls and procedures to ensure completeness and accuracy of information during the collection, storage, processing and presentation of information and data, and protection from any unauthorized modification or destruction.

Privacy: Establishing controls and procedures to ensure that information is made available or disclosed to authorized institutions or individuals only.

Accountability: Establishing controls and procedures to ensure accountability for information and actions taken by data providers and users.

Identity Verification: Confirming the identity of the data recipient or data deliverer and verifying that he is authorized to receive or deliver the data. It also includes verifying that any data request message sent is a real message that came from the original source and has not been subjected to any change or alteration.

Non-denial: Ensuring that the recipient does not deny receiving this data or information, and a method must be used to prove that the receiving person is an authorized person and bears his signature and data, as well as the data of the person submitting this data.

Authorities: Ensuring that the authorities given to certain persons are allowed to exchange or obtain certain information at a specific time and with specific powers by the direct supervisor.

Information security audit for handover and receipt: It is the recording of all events and processes that take place regarding the delivery and receipt of data, determining the size of files and the times of receipt and delivery, and examining the received data before handing

it over to the laboratory to ensure that it is free of malicious files.

Develop appropriate and detailed procedures for implementing security: including providing awareness and training in the field of information security for those associated with the electronic census project.

Project resources (including but not limited to e-mail and the Internet) are intended for functional use and must be used for work purposes only.

Ownership of all information stored or transmitted through the project resources of the E-Census 2020 project and has the right to monitor and audit it. They must be identified and appropriately classified.

Providing an Information Security Policy: These procedures and guidelines are provided in the Census' private offices and for all project personnel.

Review the Information Security Policy, supporting policies, guidelines and procedures every 6 months.

Monitor compliance with the Policy on a regular basis, information assets and the mechanism for their use will be monitored.

- Access to project resources and information shall be on at the basis of "knowledge as needed".
- An Information Security Officer(s) should be appointed to coordinate the implementation of all relevant security policies, initiatives and tasks.
- The Information Security Responsible will ensure that security issues are addressed and a mechanism is put in place to prevent their recurrence in the future.
- When information is transferred into or out of the project, special measures must be taken to secure it.
- Software and websites developed or used in an electronic census project must undergo appropriate security approval before moving into the display and use environment.
- The Electronic Census Project reserves the right to monitor the movement of information and all communications regardless of the medium used.
- The project network must be adequately protected using appropriate hardware and software.

They should be monitored and verified on a regular basis and regular checks are performed on the network, servers, and other equipment to ensure that the network is secure.

- To protect against anticipated threats to the e-census project, appropriate safeguards must be in place, including anti-virus software, firewalls, intrusion prevention systems (IPS), and other technical requirements commensurate with the sensitivity and importance of the project.
- Using the unified government network to communicate between government institutions in a secure manner.
- All documents in the project must have a version number with the document number and all pages must be numbered.
- All actual or suspicious security incidents, vulnerabilities, and information security breaches must be reported and investigated by the project's information security team.
- Disciplinary action may be taken as provided for by the laws and regulations on which this document is based.
- The information security incident response team shall have a documented emergency response plan that includes all necessary procedures.
- Proper checking of all systems should be done on a regular basis with the help of penetration testing, physical security and social engineering. A semi-annual information security audit should be conducted to verify the effectiveness of implementation controls. The audit report is reviewed by the management and appropriate measures taken to enhance security within the 2020 Census Project on an ongoing basis.
- Material security is central. All efforts should be made to secure the material perimeter, material entry points, office rooms, laboratories and server rooms using the access card and fingerprint. Take appropriate measures to secure all equipment, power supplies and cables.
- Equipment and devices must be secured during their maintenance outside the scope of the project.
- All project personnel, corporate employees and visitors must wear their identification badges and ensure that they are visible at all project facilities.
- It is strictly prohibited to discuss sensitive information (individual, population, residences,

facilities) in public, or even talking about it to those who have nothing to do with the project.

- All job advertisements and tenders must be carefully reviewed, so as not to disclose any information outside the permitted limits.
- If a project employee presents a working paper, a presentation, or delivers a speech at a public forum or conference, all materials must be reviewed by the person directly responsible for it, and then written approval is obtained from the Director General of the Electronic Census Project.
- The e-census project must comply with all legal requirements set by the Government of the Sultanate of Oman and employees must not indulge in an activity that is illegal under local or international law.
- All concerned shall ensure compliance with this Policy, and the other policies included in the manual of Controls, Standards, Procedures, Guidelines and relevant detailed Policy (outside this Handbook).

1.4 Responsibilities

Everyone who works with the E-Census 2020 project is responsible, according to their specialty, to effectively implement an information security policy, including appropriate data collection, storage and processing. Each team dealing with personal data must ensure that it is handled and processed in line with the principles and policy of data protection.

1. **The Information Security Officer** will ensure that principles, guidelines, and procedures are applied to implement this policy, and will be responsible for an ongoing review of its effectiveness and ensuring that all employees are fully aware of their obligations and responsibilities.

2. **The Information Security Officer** requires all employees, whether they are contracted E-Census 2020 project employees, project teams in government and private organizations, people involved with the work of the project or visitors, to comply with the Information Security Policy.

3. **Managers are responsible** for maintaining the data and other information assets that support project activities and under their supervision to ensure those assets are adequately secured. They must also ensure that information security guidelines and procedures are adhered to in the performance of these activities.

4. **The Information Security Officer** is responsible for the day-to-day management of information security procedures and practices. He reports directly to the Director General.

5. **Director General of the Census** is responsible for ensuring the implementation of the security policy in the project.

6. **The project management** and analysis team are responsible for:

- Keeping the Director General informed about data protection responsibilities.
- Reviewing all relevant data protection procedures and policies, in line with an agreed schedule.
- Ensuring that data is appropriately collected, stored and processed.

7. **Data Collection Team:**

- Authorized to collect data is given to specific people who are allowed to transfer or obtain certain information at a specific time and with specific powers by the census administration.
- The necessary data is requested for the statistical purposes of the census only.
- Ensure that all systems, services and equipment used for data storage meet acceptable security standards in accordance with the proposed policy.
- Conduct regular checks and surveys in cooperation with specialized technicians to ensure that security devices and programs are working properly.
- Cooperating with donors by answering their inquiries in case they have questions.

- All individual data is received only through e-mail (ecensus.data@ncsi.gov.om). The data is protected with a secret number.
- Employees should seek assistance from their line director if they are unsure of any aspect of data protection.
- A team consisting of two people is formed to receive the data, and it is not delivered in the absence of both of them.

8. Data Donors:

- Dealing with requests received from the census project staff to know or obtain data or obtain statistics.
- Alert the data collection team of important updates and modifications to the data.
- Ensure the identity of data collector or the request sent by e-mail before submitting the data. All individual data is sent only through e-mail (ecensus.data@ncsi.gov.om). The data is protected with a secret number.
- Ensure that data is transferred to reliable and encrypted devices and that the data is encrypted before it is transferred. The data receiver is not given the password directly, but rather it is sent to the e-mail (ecensus.data@ncsi.gov.om).
- Verify that any data request message sent is a real message that came from the original source and that there has been no change or alteration.

9. Director of Population Database and Director of Facilities Database are responsible for:

- Suggesting the names of the personnel assigned to receive the data; to obtain the approval of the Director General, assuring them of taking all necessary measures for data integrity.
- Evaluating the services of any third party that the project wishes to use its services to view the data.
- Dealing with data protection questions from employees and others covered by this policy.
- Contributing to the implementation of the information security policy and data protection for the persons covered by this policy.

10.Media Director is responsible for:

- Respond to any inquiries about data protection from journalists or media outlets such as newspapers and social media.
- Work with other employees to ensure that marketing and media initiatives adhere to data protection principles.
- Preventing the submission of any media statement regarding the electronic census project 2020 by any employee or contractor with the project before obtaining the approval of the Director General.

1.5 violation

In the event of violation of policy, guidelines or procedures, legal action will be taken as stipulated by the laws in the State.

1.6 Responsibility

All E-Census 2020 contract employees and project teams in government and private institutions and people associated with business with the project.

2 | Acceptable Use Policy:

2.1. The Purpose: the purpose of the Acceptable Use Policy is to communicate the minimum that all participants in the Electronic Census Project 2020 must know to ensure the security of systems, assets and information.

2.2 The Range: covers the scope of this policy. All E-Census 2020 contract employees and project teams in government and private institutions and people associated with work of the project.

2.3 Policy

- Information Security is a process shared by everyone and is everyone's daily responsibility. Everyone must contribute to the implementation of the security policy laid down in the Electronic Census 2020 project.
- Project resources (including but not limited to e-mail and the Internet) are intended for functional use only.
- Following the instructions issued by the Information Security Officer from time to time.
- All information stored or transmitted through project resources is the property of the E-Census 2020 project. The E-Census 2020 project has the right to monitor its use.
- Reproduction or transfer of information is prohibited except when necessary for work and with a prior permission from Director General of the project for those concerned only.
- All employee passwords and passphrases must be protected. He should not share it with anyone else.
- Password must be changed according to the password policy. Passwords may not be left written in an accessible place.
- All desktop and laptop computers must have a password-protected screen saver and be activated after no more than 3 minutes of non-use.
- Ensuring that there are no individual data stored in the work laptop and used outside the laboratories, all individual data is stored in private and protected servers.
- Disabling and deactivating the virus detection engine is prohibited.
- Email and Internet policy must be followed while using email or the Internet.
- Port scanning and port scanning of servers is prohibited unless it is part of an official penetration test performed by an enumeration project and appropriate measures are taken.
- Ensuring that all information of individuals, residences and establishments, printed as a hard copy or in electronic form, is kept securely.
- It is strictly prohibited to take out the project's computer outside the scope of the project, in addition; it is prohibited to take out any project statistics, reports or definitions without obtaining prior permission.
- Understanding and following the information security policy is the individual responsibility of all project personnel.

3 | Security Awareness Policy:

3.1. The Purpose:

The purpose of this policy is to keep employees informed of information security changes.

3.2. The Range:

The policy applies to all seconded permanent/contract employees, consultants and consulting firms of the E-Census 2020 project.

3.3. Policy:

- The Information Security Officer organizes one workshop at least every 6 months and the attendance of each employee will be mandatory.
- The Information Security Policy will be introduced to the security awareness of each new employee or company that joins to work within the scope of the project through a "pledge" which needs to be signed by the employee.
- It is the responsibility of each individual to educate himself and update his security information by reading and participating in the security trainings and workshops conducted by the census project.
- Any security breach or security inquiry must be reported immediately to the Information Security Officer.
- Knowledge of security policy is one of the areas in which the employee will be evaluated.

3.4 Violation

In the event of violation of the policy, guidelines or procedures, legal action will be taken as stipulated by the laws in the country.

3.5. Responsible

Information Security Officer, Information Security Auditor (internally and externally).

Conclusion:

Information security, often referred to as (InfoSec), refers to the processes and tools designed and used to protect all types of information. It is a process shared by everyone and the responsibility of everyone on a daily basis. Therefore, everyone must contribute to the implementation of the security policy set by the management of the electronic census project, represented in defining the administrative foundations, support, and commitment of information security initiatives in the electronic census project 2020. This policy also defines acceptable practices regarding the use of E-Census 2020 information resources including but not limited to, data, computing equipment, software, network services, e-mail, Internet/intranet and other media, and storage. In addition, this policy contains the minimum that every employee should know. This policy informs employees that information security is everyone's responsibility and that everyone is required to learn about information security and attend information security events/trainings/ workshops.

Through all the statistical operations and treatments that took place in the laboratories and the roles played by all the committees and teams, the security policy set by the project management has achieved its results with high accuracy by maintaining the confidentiality of data and information. Ensuring that all systems, services and equipment used to store data meet the accepted security standards. In accordance with the proposed policy, and to ensure protection against the expected threats of the electronic census project, and to provide appropriate safeguards, including anti-virus software, firewalls, intrusion prevention systems (IPS) and other technical requirements commensurate with the sensitivity and importance of the project.

E-Census Documents
Series 2020