Date: 10 January 2024 **Authors:** Cecilia Colasanti (Istat, Italia), Vadimas Ivanovas (Statistics Lithuania) and representatives staff members from Department of Statistics, Jordan. **Status:** Draft	**التاريخ:** 10 يناير 2024 **المؤلفين:** سيسيليا كولاسانتي (الإحصاءات الإيطالية)، فاديماس إيفانوفاس (الإحصاءات اللتوانية) وممثلون من دائرة الإحصاءات العامة الأردنية **الحالة:** مسودة
The Information Security Policy of Jordan's Department of Statistics	**سياسة أمن المعلومات لدائرة الإحصاءات العامة الأردنية**
1. Introduction The Information Security Policy of Department of Statistics of the Hashemite Kingdom of Jordan (DoS) establishes the general principles to be applied by DoS to the assets managed under the ISMS (Information Security Management System), following ISO/IEC 27001:2022 standard as well as the Jordan applicable legislation and regulations (Law on Statistics and Information Security). In the next review of this policy (if necessary) it is possible to introduce also other standards and frameworks.	**1. المقدمة** تحدد سياسة أمن المعلومات التي سوف تتبعها دائرة الإحصاءات العامة بالمملكة الأردنية الهاشمية المبادئ العامة التي تطبقها الدائرة على الأصول التي تدار بموجب نظام إدارة أمن المعلومات، وفقا لمعيار ISO/IEC 27001:2022، فضلا عن التشريعات واللوائح المعمول بها في الأردن (قانون الإحصاءات وأمن المعلومات). وفي المراجعة المقبلة لهذه السياسة (إذا لزم الأمر) يمكن أيضا إدراج معايير وأطر أخرى.
When establishing the ISMS, the DoS top management assumes this policy, the commitments defined therein, the integration of the ISMS requirements in the organization's processes and ensures that the necessary resources for its implementation are available. It has the responsibility towards the interested parties to act appropriately regarding information security management, as well as to monitor and assess the implementation of the ISMS.	وعند إنشاء نظام إدارة أمن المعلومات، تتولى الإدارة العليا لدائرة الإحصاءات العامة هذه السياسة، والالتزامات المحددة فيها، وإدماج متطلبات هذا النظام في عمليات المؤسسة، وضمان توافر الموارد اللازمة لتنفيذه. وهي مسؤولة تجاه الأطراف المعنية عن التصرف على النحو المناسب فيما يتعلق بإدارة أمن المعلومات، فضلا عن رصد وتقييم تنفيذ نظام إدارة أمن المعلومات.
This policy is aligned with the government strategy (see paragraph 2)	تتماشى هذه السياسة مع استراتيجية الحكومة (انظر الفقرة 2)
Whenever it refers to information security management, in the context of DoS, it should be considered that it also covers the Personal Data Protection Law (24/2023).	وعندما تشير إلى إدارة أمن المعلومات، في سياق دائرة الإحصاءات العامة، ينبغي اعتبار أنها تشمل أيضا قانون حماية البيانات الشخصية (2023/24).

2. DoS undertakes to:	2. تلتزم دائرة الإحصاءات العامة بما يلي:
Comply with legal requirements and other relevant national and international standards on information security. It will be listed below, among others: • General Principles and Regulation of Electronic Participation; • The National strategy for cyber security 2018-2023; • The National strategy for ensuring and guaranteeing cyber security and information security (2012) • Cyber security policy (2019); • Policy of the use IT resources in the ministry of Digital economy (2023) • Government data classification policy (2020); • Law guarantee the right to access information (47/2007);	الامتثال للمتطلبات القانونية وغيرها من المعايير الوطنية والدولية ذات الصلة بأمن المعلومات. وسترد أدناه، من بين أمور أخرى: • المبادئ العامة وتنظيم المشاركة الإلكترونية؛ • الاستراتيجية الوطنية للأمن السيبراني 2018-2023؛ • الاستراتيجية الوطنية لضمان الأمن السيبراني وأمن المعلومات (2012) • سياسة الأمن السيبراني (2019)؛ • سياسة استخدام موارد تكنولوجيا المعلومات في وزارة الاقتصاد الرقمي (2023) • سياسة تصنيف البيانات الحكومية (2020)؛ • قانون ضمان الحق في الحصول على المعلومات (2007/47)؛
Ensure the confidentiality, integrity and availability of information in its processes;	ضمان سرية المعلومات وسلامتها وتوافرها في عملياتها؛
Ensure effective communication of information security policies and procedures;	ضمان التواصل الفعال فيما يتعلق بالسياسات والإجراءات بشأن أمن المعلومات؛
Implement a continuous process of information security awareness-raising and training;	تنفيذ عملية مستمرة للتوعية والتدريب في مجال أمن المعلومات؛
Demonstrate to be a secure organization with regard to information security.	إثبات أنها منظمة آمنة فيما يتعلق بأمن المعلومات.

3. Scope

The Information Security Policy of DoS is available to all stakeholders (among others, employees, contractors, suppliers, volunteers other organizational bodies and anyone who has permanent or temporary access to DoS information or systems).

All stakeholders must know and act in accordance with the Information Security Policy of DoS and with the other documents related to Information Security, as applicable and appropriate. All stakeholders covered by the ISMS who deliberately breach this or other policies are subject to sanctions and other actions, as applicable, up to and including termination of contract and/or reporting to the concerned authorities for criminal offences.

4. Value of information

Information may take various forms (printed or written on paper, stored electronically, transmitted by mail or electronic means, among others), and must be adequately protected, regardless of its medium, use or support.

Information security should be adjusted to its importance and value.

Access to information is vital to the functioning of DoS, depending on the availability of information systems and infrastructures. Security in the processing and transmission of information is thus fundamental to the efficiency of the process of producing official statistics.

Any interruption of service, leak of information to unauthorized entities or unauthorized modification of data may lead to a loss of trust and/or breach legal and contractual obligations towards citizens and companies.

3. النطاق (الرؤية)

وسياسة أمن المعلومات التي سوف تتبعها دائرة الإحصاءات العامة متاحة لجميع أصحاب المصلحة (من بينهم الموظفون والمتعاقدون والموردون والمتطوعون والهيئات التنظيمية الأخرى وأي شخص لديه إمكانية دائمة أو مؤقتة للوصول إلى معلومات أو نظم دائرة الإحصاءات العامة).

ويجب على جميع أصحاب المصلحة أن يعرفوا سياسة أمن المعلومات التي تتبعها دائرة الإحصاءات العامة والوثائق الأخرى المتصلة بأمن المعلومات وأن يتصرفوا وفقا لها، حسب الاقتضاء. ويخضع جميع أصحاب المصلحة المشمولين بنظام إدارة أمن المعلومات الذين ينتهكون عمدا هذه السياسات أو غيرها لعقوبات وإجراءات أخرى، حسب الاقتضاء، حتى إنهاء العقد و/أو إبلاغ السلطات المعنية بالجرائم الجنائية.

4. قيمة المعلومات

ويمكن أن تتخذ المعلومات أشكالا مختلفة (مطبوعة أو مكتوبة على الورق، مخزنة إلكترونيا، مرسلة بالبريد أو بوسائل إلكترونية، وغير ذلك)، ويجب أن تحظى بحماية كافية، بصرف النظر عن وسطها أو مجال استخدامها أو دعمها.

وينبغي تعديل أمن المعلومات استنادا إلى أهمية وقيمة المعلومات.

والوصول إلى المعلومات أمر ضروري لعمل دائرة الإحصاءات العامة، رهنا بتوافر نظم المعلومات والهياكل الأساسية. وبالتالي، فإن الأمن في معالجة المعلومات ونقلها أساسي لكفاءة عملية إنتاج الإحصاءات الرسمية.

وأي انقطاع في الخدمة أو تسرب معلومات إلى كيانات غير مأذون لها أو تعديل غير مأذون به للبيانات قد يؤدي إلى فقدان الثقة و/أو خرق الالتزامات القانونية والتعاقدية تجاه المواطنين والشركات.

It is the responsibility of all stakeholders to proactively contribute to information security. Additionally, it should be noted that official statistics depends on the correct and expected functioning of the information and communication systems of DoS in order to achieve its objectives on information security. However, this is only possible with the continuous identification of the risks to which the assets, namely under the responsibility of DoS, are exposed, and by implementing security controls and mechanisms aimed at their correct and controlled use.	وتقع على عاتق جميع أصحاب المصلحة مسؤولية الإسهام بصورة فعالة في أمن المعلومات. وبالإضافة إلى ذلك، تجدر الإشارة إلى أن الإحصاءات الرسمية تعتمد على الأداء الصحيح والمتوقع لنظم المعلومات والاتصالات في دائرة الإحصاءات العامة من أجل تحقيق أهدافها المتعلقة بأمن المعلومات. ومع ذلك، لا يمكن تحقيق ذلك إلا من خلال التحديد المستمر للمخاطر التي تتعرض لها الأصول، أي تحت مسؤولية دائرة الإحصاءات العامة، ومن خلال تنفيذ ضوابط وآليات أمنية تهدف إلى استخدامها السليم والذي ينم ضبطه.
5. Value of information security The information managed by DoS, its support processes, systems, applications and networks are valuable assets to society. The guarantee of confidentiality, integrity and/or availability of information ensures the credibility of the services provided by DoS. Information security shall therefore be applied in all phases of the life cycle of the activities pursued by DoS. The information security control of the insertion / collection, processing, storage, transfer, relationship, search and destruction operations of information is as important as or more important than the functionality of an information system.	5. قيمة أمن المعلومات وتعتبر المعلومات التي تديرها دائرة الإحصاءات العامة وعمليات الدعم والنظم والتطبيقات والشبكات التابعة لها أصولا قيمة للمجتمع. ويكفل ضمان سرية المعلومات و/أو سلامتها و/أو توافرها مصداقية الخدمات التي تقدمها دائرة الإحصاءات العامة. ولذلك يطبق أمن المعلومات في جميع مراحل دورة حياة الأنشطة التي تضطلع بها دائرة الإحصاءات العامة. ومراقبة أمن المعلومات المتعلقة بإدراج/جمع المعلومات وتجهيزها وتخزينها ونقلها وعلاقتها بالعمليات والبحث عنها وتدميرها لا تقل أهمية أو أكثر أهمية عن وظيفة نظام المعلومات.

Thus, the permanent and balanced maintenance of a high level of quality and security must be ensured, preventing the materialization of inherent risks in order to mitigate/limit the potential damage caused by the exploitation of vulnerabilities and information security incidents. Information security threats are constantly evolving, which implies the continuous adaptation of information security measures to keep up with technological and legislative or regulatory changes. Information security measures shall be technically and economically feasible and shall not limit the efficiency of DoS.	وبالتالي، يجب ضمان الحفاظ الدائم والمتوازن على مستوى عال من الجودة والأمن، مما يحول دون تجسيد المخاطر الكامنة من أجل تخفيف/الحد من الضرر المحتمل الناجم عن استغلال نقاط الضعف وحوادث أمن المعلومات. وتتطور التهديدات المتعلقة بأمن المعلومات باستمرار، مما يعني استمرار تطويع تدابير أمن المعلومات لمواكبة التغييرات التكنولوجية والتشريعية أو التنظيمية. تكون تدابير أمن المعلومات مجدية من الناحيتين التقنية والاقتصادية ولا تحد من كفاءة دائرة الإحصاءات العامة.
6. Guidelines for Information Security Management	6. المبادئ التوجيهية لإدارة أمن المعلومات
People management: the Information Security Policy is applicable to all users of DoS, as defined in chapter 3, and shall be applied across the board in all organizational structures, with specific responsibilities being established for certain functions;	***إدارة الأفراد***: تنطبق سياسة أمن المعلومات على جميع المستخدمين في دائرة الإحصاءات العامة، على النحو المحدد في الفصل 3، وتطبق في جميع الهياكل التنظيمية، مع تحديد مسؤوليات محددة لمهام معينة
Risk management: all systems (existing or planned), processes, documentation, equipment and each other asset must have an information security level appropriate to the risk to be assumed by DoS;	***إدارة المخاطر:*** ويجب أن يكون لجميع النظم (القائمة أو المخطط لها) والعمليات والوثائق والمعدات والأصول الأخرى مستوى لأمن المعلومات يتناسب مع المخاطر التي تتعرض لها دائرة الإحصاءات العامة؛
Definition of responsibilities: DoS is responsible for the quality, accesses, use and safeguarding of the information contained in the systems, processes, documentation, equipment and each other asset. DoS shall define the standards and procedures that implement the information security levels defined by the entities that own the information and monitor their effectiveness;	***تحديد المسؤوليات:*** وتتولى دائرة الإحصاءات العامة مسؤولية جودة المعلومات الواردة في النظم والعمليات والوثائق والمعدات والأصول الأخرى والوصول إليها واستخدامها وحمايتها. تحدد الدائرة المعايير والإجراءات التي تنفذ مستويات أمن المعلومات التي تحددها الكيانات التي تمتلك المعلومات وترصد فعاليتها؛

Information security policies: there should be detailed information security policies applicable to all information systems, processes, documentation, equipment and each other asset, regardless of their environment;	***سياسات أمن المعلومات:*** وينبغي أن تكون هناك سياسات مفصلة لأمن المعلومات تنطبق على جميع نظم المعلومات وعملياتها ووثائقها ومعداتها وأصولها الأخرى، بصرف النظر عن بيئتها؛
Information security procedures: there should be procedures as detailed as possible defining "what" and "how" to achieve the desired level of information security, as well as defining the level of human involvement in information systems maintenance;	***إجراءات أمن المعلومات***: ينبغي أن تكون هناك إجراءات مفصلة قدر الإمكان تحدد "ماذا" و "كيف" لتحقيق المستوى المطلوب من أمن المعلومات، فضلا عن تحديد مستوى المشاركة البشرية في استدامة نظم المعلومات؛
Traceability of information systems: operations on information systems should be properly documented, ensuring that at any time it is possible to ascertain "who" and "when" did "what";	***إمكانية تتبع نظم المعلومات:*** ينبغي توثيق العمليات المتعلقة بنظم المعلومات توثيقا سليما، بما يكفل إمكانية التحقق في أي وقت من "من" و "متى" فعل "ماذا"؛
Monitoring of controls: the implementation of controls that address the risks to which the business is exposed can only be effective if there is adequate monitoring of the controls, in order to assess if they are adjusted to the defined objectives. Timely response actions must also be defined in the event of non-operational controls.	***مراقبة الضوابط:*** لا يمكن أن يكون تنفيذ الضوابط التي تعالج المخاطر التي تتعرض لها المؤسسات فعالا إلا إذا كان هناك رقابة كافية للضوابط، من أجل تقييم ما إذا كانت معدّلة وفقا للأهداف المحددة. ويجب أيضا تحديد إجراءات الاستجابة في الوقت المناسب في حالة وجود ضوابط غير تشغيلية.

7. Information Security Management System

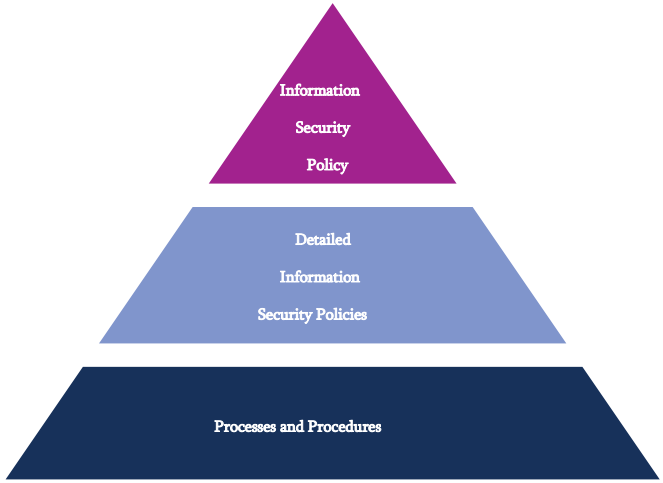
The ISMS model of DoS is based on three vectors:

Confidentiality: guarantee that the information is accessible only to users and external entities duly authorized for that purpose;

Integrity: safeguard the accuracy of information and processing methods;

Availability: guarantee that authorized users have access to the information whenever necessary.

All information security mechanisms existing in DoS aim at the confidentiality, integrity and/or availability of information, and shall be regulated by a set of detailed information security policies, processes and procedures, structured as follows:



7. نظام إدارة أمن المعلومات

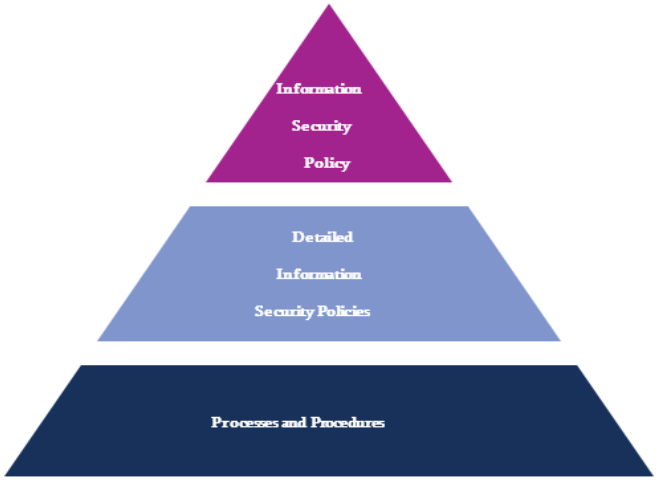
يستند نموذج نظام إدارة أمن المعلومات في دائرة الإحصاءات العامة على ثلاث محاور رئيسية:

السرية: ضمان ألا يتاح الوصول إلى المعلومات إلا للمستخدمين والكيانات الخارجية المأذون لها بذلك على النحو الواجب؛

سلامة المعلومات: والحفاظ على دقة المعلومات وأساليب المعالجة؛

الإتاحة (التوافر): ضمان حصول المستخدمين المأذون لهم على المعلومات عند الاقتضاء.

تهدف جميع آليات أمن المعلومات الموجودة في دائرة الإحصاءات العامة إلى الحفاظ على سرية المعلومات و/أو سلامتها و/أو توافرها، وتنظمها مجموعة من السياسات والعمليات والإجراءات التفصيلية المتعلقة بأمن المعلومات، على النحو التالي:



Detailed information security policies	السياسات التفصيلية لأمن المعلومات:
1. Access control – physical, digital (hardware and software) and organizational.	1. التحكم بالوصول – المادي، الرقمي (المعدات والبرمجيات) والتنظيمي
2. Statistical confidentiality (public)	2. السرية الإحصائية (عامة الجمهور)
3. Confidentiality classification of information	3. تصنيف السرية للمعلومات
4. Physical and environmental safety	4. الأمن البيئي والمادي
5. Continuity and Backups	5. الاستمرارية والنسخ الاحتياطية
6. Transfer of information	6. نقل المعلومات
7. Malware protection	7. الحماية من البرامج الضارة
8. Event or incident management	8. إدارة الأحداث
9. Cryptographic controls	9. ضوابط التشفير
10. Communications security	10. أمن الاتصالات
11. Privacy and protection of personal data (public)	11. خصوصية وحماية البيانات الشخصية (عامة الجمهور)
12. Safe development	12. التطوير الآمن
13. Software management	13. إدارة البرمجيات
14. Amendment control and change management	14. مراقبة عمليات التعديل وإدارة التغيير
15. Relations with suppliers	15. العلاقات مع الموردين
16. Acceptable use of assets	16. الاستخدام المقبول للأصول
17. Use of removable data devices	17. استخدام أجهزة البيانات القابلة للإزالة
18. Clean desk and screen	18. مكتب نظيف والشاشة
19. Mobile devices and teleworking	19. الأجهزة المحمولة والعمل عن بُعد
20. Project management	20. إدارة المشاريع
21. Acceptable use of communication and collaboration platforms	21. الاستخدام المقبول لمنصات التواصل والتعاون
Procedures	الإجراءات
1. Risk and opportunity management	1. إدارة المخاطر والفرص
2. Capacity management	2. إدارة القدرات والكفاءات
3. Continuity management	3. إدارة الاستمرارية
4. Non-compliances and corrective actions	4. عدم الامتثال والإجراءات التصحيحية
5. Documentary control	5. التحكم الوثائقي
6. Internal Audits	6. عمليات التدقيق والمراجعات الداخلية
7. Operations	7. العمليات
8. Management Review	8. المراجعة الإدارية
9. Procedure for disposal and reuse of data media and equipment	9. إجراءات التخلص من وسائط ومعدات البيانات وإعادة استخدامها

8. Organization of Information Security *[not discussed]* The organization of information security aims at establishing, implementing, maintaining and continuously improving the ISMS in the context of the organization and specifies the requirements for the assessment and processing of information security risks according to the needs of DoS. The ISMS's management structure is made up of: The DoS top management, which is responsible for monitoring and assessing the implementation of the ISMS; The Information Security Officer of DoS, which is responsible for managing the ISMS; The Data Protection Officer which actively participates in the development of the ISMS, especially in the Privacy and Data Protection Policy and on issues with implications on personal data protection; The Information Security Team of DoS, that includes different skills and employees coming from IT directorate of DoS, is responsible for implementing information security mechanisms.	8. تنظيم أمن المعلومات *(لم يناقش بعد)* يهدف تنظيم أمن المعلومات إلى إنشاء وتنفيذ واستدامة وتحسين نظام إدارة أمن المعلومات ISMS باستمرار في سياق المنظمة ويحدد متطلبات تقييم ومعالجة مخاطر أمن المعلومات وفقًا لاحتياجات دائرة الإحصاءات العامة. يتكون هيكل نظام إدارة أمن المعلومات ISMS من: الإدارة العليا لدائرة الإحصاءات العامة، التي تعد مسؤولة عن مراقبة وتقييم تنفيذ نظام إدارة أمن المعلومات؛ ضابط أمن المعلومات في دائرة الإحصاءات العامة، الذي يكون مسؤولا عن إدارة نظام ISMS ضابط حماية البيانات الذي يشارك بشكل فعال في تطوير نظام ISMS، خصوصا فيما يتعلق بالخصوصية وسياسة حماية البيانات وفي المسائل التي تؤثر على حماية البيانات الشخصية. ويضطلع فريق أمن المعلومات التابع لدائرة الإحصاءات العامة، الذي يضم مهارات وموظفين مختلفين من مديرية تكنولوجيا المعلومات في الدائرة، بمسؤولية تنفيذ آليات أمن المعلومات.

9. Maintenance and communication of security policies and procedures Information security policies and procedures shall be known to all stakeholders, as mentioned in the chapter 3, within their scope of application, and effective communication of the policies and procedures shall be ensured so that stakeholders are aware of their individual obligations in relation to information security. Information security policies and procedures are regularly revised, ensuring that they remain relevant and appropriate. The ISMS is subject to assessment audits through internal audit and by independent audit entities (as example, among others, Bureau Veritas).	9. **الحفاظ على السياسات والإجراءات الأمنية والإبلاغ عنها** يجب أن تكون السياسات والإجراءات المتعلقة بأمن المعلومات معروفة لجميع أصحاب المصلحة، على النحو المذكور في الفصل 3، ضمن نطاق تطبيقها، ويجب ضمان التواصل الفعال بما يتعلق بالسياسات والإجراءات بحيث يكون أصحاب المصلحة على علم بالتزاماتهم الفردية فيما يتعلق بأمن المعلومات. ويجري بانتظام مراجعة السياسات والإجراءات المتعلقة بأمن المعلومات، بما يكفل استمرار أهميتها وملاءمتها. ويخضع هذا النظام لعمليات مراجعة وتدقيق تقييمية من خلال المراجعة الداخلية ومن قبل كيانات مستقلة للمراجعة والتدقيق (مثل مكتب فيريتاس).