

سياسة أمن و سلامة المعلومات Information Security Policy Statement

Municipality & Planning Department - Ajman is committed to safeguard its intellectual property, AM - ITD infrastructure and stakeholders' information with regard to Information Technology Services provided by the Municipality. Municipality and Planning Department - Ajman (MPDA) intends to provide the highest level of protection possible to all aspects of information flowing through its AM - ITD infrastructure. The Information Security Policy is framed around:

Availability: which assures that the processes, policies, and controls are used to ensure, only authorized users have prompt access to information. This prevents accidental attempt to access information and systems by illegitimate users and helps legitimate users access information and systems as required by the system.

Integrity: which assures that adequate processes, policies, and controls will be used to ensure that information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

Confidentiality: which assures that adequate processes, policies, and controls are employed to protect the information of customers and the institution against unauthorized access or use.

Accountability: which assures that adequate processes, policies, and controls are in place that are necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

Assurance: which assures that adequate processes, policies, and controls are used to develop confidence that technical and operational security measures work, as

The Information Security Policy of MPDA is governed and implemented as per ISO/IEC 27001:2022 standard and SOA 1.8

تلتزم دائرة البلدية والتخطيط - عجمان بحماية الملكية الفكرية والبنية الأساسية لتقنية المعلومات الخاصة بالدائرة، وحماية المعلومات الخاصة بجميع الجهات المعنية بخدمات تقنية المعلومات التي تقدمها الدائرة، لذلك تبذل الدائرة كل ما في وسعها من أجل توفير أقصى حماية ممكنة لكافة أنواع المعلومات التي تمر عبر البنية الأساسية لتقنية المعلومات، وفق هذه السياسة الخاصة بأمن وسلامة المعلومات، والقائمة على المحاور التالية:

توفر المعلومات: حيث تضمن جميع السياسات، والعمليات والضوابط المستخدمة في النظام المعلوماتي توفر المعلومات المطلوبة للأفراد المعنيين والذين لديهم صلاحية الاطلاع عليها عند الحاجة دون أي تأخير، ومنع أي محاولة للاطلاع على تلك المعلومات أو النظم المعلوماتية من قبل أي شخص غير مصرح له، سواء بطريق الصدفة أو عن قصد، وكذلك ضمان سهولة دخول الأفراد الذين لديهم الصلاحية الشرعية على النظم المعلوماتية وفق النظام المعمول به ومتطلبات العمل.

سلامة المعلومات: حيث نتأكد من وضع واستخدام سياسات وعمليات وضوابط تضمن عدم تحريف المعلومات أو تدليسها بطريقة غير مسؤولة، وتضمن النظم المعلوماتية عدم التلاعب في المعلومات بطريقة غير مسؤولة مما يعرض دقتها أو اكتمالها أو الثقة فيها للخطر.

سرية المعلومات: حيث نتأكد من وضع واستخدام سياسات وعمليات وضوابط تحافظ على المعلومات الخاصة بالمعاملين والدائرة من الاطلاع عليها أو استخدامها من قبل أي شخص ليست لديه الصلاحية.

المساءلة: حيث نتأكد من وضع واستخدام السياسات والعمليات والضوابط اللازمة لتتبع الإجراءات حتى مصدرها، فالمساءلة تدعم عدم التنصل من المسؤولية، والردع، ومنع اختراق الأنظمة المعلوماتية، ومراقبة أمن المعلومات، واسترجاع المعلومات، وقانونية قبول السجلات.

الضمان (التأكيد): حيث نتأكد من وضع السياسات والعمليات والضوابط اللازمة واستخدامها لرفع مستوى الثقة في كفاءة ضوابط الأمن التقني والتشغيلي، وأنها تعمل وفق ما هو منشود، وتعتبر مستويات التأكيد جزء من تصميم النظام.

تم وضع هذه السياسة والالتزام بها وفق المواصفة الدولية للأيزو

27001:2022 والوثيقة SOA V.18

Document V 1.8	Data: 23-5-2024	Document Classification: Public	التصنيف: عام	التاريخ: 23-5-2024	إصدار الوثيقة: V 1.8
-------------------	--------------------	------------------------------------	-----------------	-----------------------	-------------------------