هـيـئـة Digital
الحكومة Government
الرقمية Authority

ضوابط حوكمة تقنية المعلومات في الحكومة الرقمية

نوفمبر 2025

نـــوع الوثيقـــة: ضوابط
تصنيف الوثيقة: عام
رقـــم الإصـــدار: 2.0
رقـــم الوثيقـــة: DGA-1-2-5-108

المحتويات

1. تمهيد

تعمل هيئة الحكومة الرقمية على تعزيز الأداء الرقمي داخل الجهات الحكومية، والرفع من جودة الخدمات المقدمة، وتحسين تجربة المستفيد من تلك الخدمات، بما يتوافق مع الرؤية الطموحة للمملكة العربية السعودية (2030)، وتحقيق التوجهات الإستراتيجية للحكومة الرقمية.

وتُمهّد هيئة الحكومة الرقمية الطريق للجهات الحكومية، لتوفير خدمات حكومية رقمية ذات جودة وكفاءة عالية تُسهم في رفع العوائد الاستثمارية وقيمة الاقتصاد الوطني، كما تعمل الهيئة على قياس أداء الجهات الحكومية وقدراتها في مجال الحكومة الرقمية، حيث إن الهيئة هي الجهة المختصة بكل ما يتعلق بالحكومة الرقمية، وتُعدّ المرجع الوطني في شؤونها، وبناء على اختصاصاتها بأن تتولى الهيئة "وضع المعايير الفنية لنماذج التحول الرقمي في القطاعات الحكومية ومتابعة الالتزام بها".

ومن هذا المنطلق أعدت الهيئة "ضوابط حوكمة تقنية المعلومات في الحكومة الرقمية"؛ لدعم حوكمة الإدارات المشرفة على تقنية المعلومات في الجهات الحكومية والإطار التنظيمي التابع للجهة، وتوحيد السياسات والإجراءات، ومتابعة الالتزام بها، وفق منهجية محددة تعزز أداء بيئة رقمية فعالة ومرنة، ودعم تنفيذ خارطة طريق التحول الرقمي للجهات الحكومية، عن طريق تحديد الأولويات بفاعلية، وتخصيص الأصول الرقمية والتقنية واستغلالها بصورة فعالة، ودعم استدامة أعمال الجهة الحكومية.

2. مقدمة

سعياً إلى تعزيز الخدمات الحكومية الرقمية في الجهات الحكومية، وقدرتها على دعم الأهداف الاستراتيجية للحكومة الرقمية، أصدرت الهيئة هذه الوثيقة؛ لضمان حوكمة عمليات تقنية المعلومات، وتعزيز آليات صنع القرار بين مسؤولي تقنية المعلومات والإدارة العليا لدى الجهة الحكومية.

وحيث يُعّد تنظيم حوكمة أعمال الإجراءات الداخلية لدى المسؤولين في تقنية المعلومات أمرًا بالغ الأهمية؛ عملت الهيئة على إعداد هذه الضوابط وتطوير إطار خاص بها، والذي تضمن خمسة مستويات رئيسة، يمثل كل مستوى منها مجموعة من الضوابط؛ بهدف المساهمة في التطبيق الفعال والمرن للضوابط، ورفع مستوى جاهزية الجهات الحكومية، وتعزيز الاستجابة للمخاطر الرقمية؛ مما يمكّن الجهات الحكومية من دعم أهدافها الإستراتيجية عن طريق تحقيق الفوائد، وتحسين مستويات المخاطر والموارد.

وجرى إعداد وثيقة " ضوابط حوكمة تقنية المعلومات في الحكومة الرقمية" وتطويرها، التي من شأنها أن تيسر تطبيق حوكمة تقنية المعلومات بفاعلية أكبر، ويجب على المسؤولين في تقنية المعلومات لدى الجهات الحكومية الامتثال لها، ويحق لهيئة الحكومة الرقمية مراقبة تنفيذها وفق الآلية المعتمدة لديها.

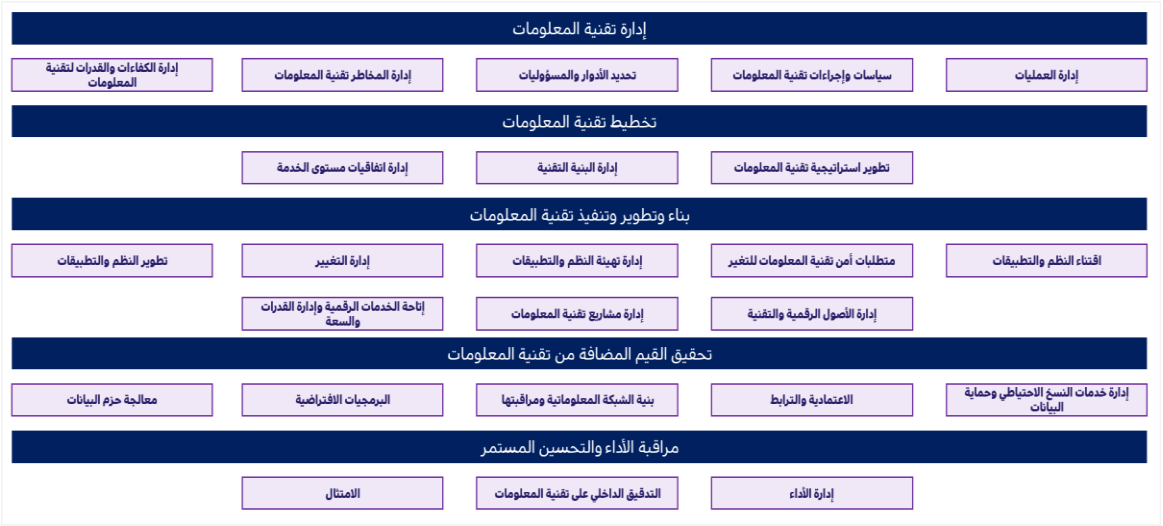
3. أهداف الضوابط

تهـدف هـذه الضـوابط إلـى تطبيـق مفهـوم حوكمـة تقنيـة المعلومـات فـي الجهـات الحكومية، وذلك عن طريق ما يأتي:

- التخطيط والتنظيم لحوكمة تقنية المعلومات، ومواءمتها مع إستراتيجيات الجهة.
- تطبيق المبادئ والممارسات السليمة لتنفيذ العمليات الخاصة بحوكمة تقنية المعلومات وتشغيلها.
- المراقبة والتقييم لمتطلبات حوكمة تقنية المعلومات الداخلية والخارجية للجهة.
- تقديم الدعم لحوكمة تقنية المعلومات وعمليات تشغيلها.

4. نطاق الضوابط

تحدد هذه الوثيقة الاشتراطات الخاصة بحوكمة تقنية المعلومات لدى الجهات الحكومية وتشمل: تنفيذ، ومراقبة، وتحسين بيئة حوكمة تقنية المعلومات داخل الجهة، وذلك وفقاً لإطار حوكمة تقنية المعلومات، والذي جرى تطويره والعمل عليه لتطبيق حوكمة تقنية المعلومات في الجهات الحكومية (الشكل 1).



الشكل (1) إطار حوكمة تقنية المعلومات

وجرى إعداد وتطوير ضوابط حوكمة تقنية المعلومات في الحكومة الرقمية بناء على خمسة مستويات رئيسة كما هو موضح في (الشكل 1)، يمثل كل مستوى مجموعة من الضوابط، وفقا لما يأتي:

1. **إدارة تقنية المعلومات، وتهدف إلى:** تمكين الإدارة العليا المسؤولة عن مستوى نضج حوكمة تقنية المعلومات لدى الجهة وفاعليتها، وتشمل الآتي:

- ضوابط إدارة العمليات.
- ضوابط سياسات وإجراءات تقنية المعلومات.
- ضوابط تحديد الأدوار والمسؤوليات.
- ضوابط إدارة مخاطر تقنية المعلومات.
- ضوابط إدارة الكفاءات والقدرات لتقنية المعلومات.

2. **تخطيط تقنية المعلومات، وتهدف إلى:** التأكيد على ضمان أن عمليات إدارة مخاطر تقنية المعلومات تُدار بفاعلية، إضافة إلى كفاءة نموذج الحوكمة والإستراتيجيات الخاصة بتقنية المعلومات،وتشمل الآتي:

- ضوابط تطوير إستراتيجية تقنية المعلومات.
- ضوابط إدارة البنية التقنية.
- ضوابط إدارة اتفاقيات مستوى الخدمة.

3. **بناء وتطوير وتنفيذ أنظمة تقنية المعلومات، وتهدف إلى:** تحديد التغييرات المتعلقة بأصول المعلومات والخدمات الرقمية وتصميمها واختبارها وتنفيذها؛ لتقليل تأثير المخاطر المتعلقة بإدارة التغيير، وتحقيق الأهداف المخطط لها، ومعالجتها عن طريق تنفيذ ضوابط تقنية المعلومات،وتشمل الآتي:

- ضوابط اقتناء النظم والتطبيقات.
- ضوابط متطلبات أمن تقنية المعلومات للتغير.
- ضوابط إدارة تهيئة النظم والتطبيقات.
- ضوابط إدارة التغيير.
- ضوابط تطوير النظم والتطبيقات.
- ضوابط إدارة الأصول الرقمية والتقنية.
- ضوابط إدارة مشاريع تقنية المعلومات.
- ضوابط إتاحة الخدمات الرقمية وإدارة القدرات والسعة.

4. **تحقيق القيم المضافة من تقنية المعلومات، وتهدف إلى:** تحقيق المنافع من بيئة تقنية المعلومات لدى الجهة، ودعم أهداف الحكومة الرقمية بتنفيذ الإدارة الفعالة والرقابة المستمرة، لذا يجب على إدارة تقنية المعلومات تطبيق الضوابط بفاعلية؛ لتقليل عوامل المخاطر المتعلقة بالعمليات التشغيلية والخدمات الرقمية، وتشمل الآتي:

- ضوابط إدارة خدمات النسخ الاحتياطي وحماية البيانات.
- ضوابط الاعتمادية والترابط.
- ضوابط بنية الشبكة المعلوماتية ومراقبتها.
- ضوابط البرمجيات الافتراضية.
- ضوابط معالجة حزم البيانات.

5. **مراقبة الأداء والتحسين المستمر، وتهدف إلى:** مراقبة الأداء وفاعلية كفاءة الخدمات الرقمية والتقنية، وضمان عملية التحسين المستمر عن طريق قياس الأداء، والقيام بالمراجعات الداخلية المستمرة، وقياس مستوى الامتثال للتنظيمات ذات العلاقة. وتشمل الآتي:

- ضوابط إدارة الأداء.
- ضوابط التدقيق الداخلي على تقنية المعلومات.
- ضوابط الامتثال.

5. تطبيق الضوابط

تطبق المتطلبات الواردة في هذه الوثيقة على:

- جميع الجهات الحكومية التي تقدّم خدمات ومنتجات رقمية.
- الجهات المشغلة لخدمات تقنية المعلومات ومزودي الخدمات الرقمية.

6. التنفيذ والالتزام

تطبيقاً لما ورد في الفقرة التاسعة من المادة الرابعة من تنظيم هيئة الحكومة الرقمية، التي نصت على أن تتولى الهيئة **"وضع المعايير الفنية لنماذج التحول الرقمي في القطاعات الحكومية، ومتابعة الالتزام بها، بالتنسيق مع الجهات المختصة"**، وبناءً عليه تُقيّم الهيئة وتقيس مدى التزام الجهات الحكومية بتطبيق هذه الضوابط وفق الآلية التي تقرّها الهيئة.

7. الضوابط

7.1 إدارة تقنية المعلومات

7.1.1 ضوابط إدارة العمليات		
الهدف	توفير الكوادر والمهارات المناسبة؛ بهدف الإشراف والتحكم في النهج العام لتقنية المعلومات داخل الجهات الحكومية.	
يجب على الجهات الحكومية أن تلتزم بما يلي:		
رقم الضابط		
5-108-01	تنشئ الإدارة العليا للجهة الحكومية لجنة داخلية توجيهية للإشراف على أعمال حوكمة تقنية المعلومات، وبما لا يتعارض مع قرار مجلس الوزراء رقم (40) وتاريخ 1427/2/27هـ، الصادر بالموافقة على ضوابط تطبيق التعاملات الإلكترونية الحكومية. على أن يتكون أعضاء اللجنة من:	
	5-108-01.01	مسؤول أول من الإدارة العليا للجهة لرئاسة اللجنة التوجيهية لتقنية المعلومات على أن يكون المسؤول الأول: • سعودي الجنسية. • ذا خبرة تتناسب مع طبيعة عمله والمسؤوليات المكلف بها.
	5-108-01.02	أن يكون المسؤول الأول أو من ينيبه لتقنية المعلومات عضواً في اللجنة.
	5-108-01.03	ممثلين من القطاعات والإدارات ذات الصلة في الجهة الحكومية.
5-108-02	وضع ميثاق اللجنة التوجيهية لحوكمة تقنية المعلومات، بعد اعتماده وتعميمه من قبل الإدارة العليا للجهة الحكومية، على أن يحتوي بحد أدنى على ما يلي:	
	5-108-02.01	أهداف اللجنة التوجيهية، وتحديد الأدوار والمسؤوليات لأعضاء اللجنة، وتوضيحها في مصفوفة الصلاحيات، باتباع مبادئ فصل المهام، وتجنب تضارب المصالح.
	5-108-02.02	تحديد عدد المشاركين الممثلين من القطاعات والإدارات في الاجتماع وآلية التصويت على القرارات.
	5-108-02.03	دورية الاجتماعات (ربع سنوي كحد أدنى)، وآلية توثيق الاجتماعات ومتابعة القرارات، على أن يشارك التقارير الدورية مع لجنة التحول الرقمي لدى الجهة.
	5-108-02.04	موثقة ومعتمدة من المسؤول الأول.
5-108-03	وضع ضوابط للأنشطة المالية المتعلقة بتقنية المعلومات، التي تغطي الميزانية، والتكلفة، وتحديد أولويات الإنفاق بما يتماشى مع الأهداف الإستراتيجية للجهة وإدارة تقنية المعلومات.	
5-108-04	مراجعة الميزانية الرئيسة لتقنية المعلومات بشكل دوري، وتعديلها وفقاً لمتطلبات تقنية المعلومات واحتياجات العمل.	
5-108-05	وضع خطة لاستقطاب وتعاقب المختصين للعمل بأقسام وإدارات تقنية المعلومات المختلفة، وتحديد الأدوار والمسؤوليات الدقيقة والحساسة داخل الجهة بالتنسيق مع إدارة الموارد البشرية.	

7.1.2 ضوابط سياسات وإجراءات تقنية المعلومات	
الهدف	إصدار سياسات وإجراءات تقنية المعلومات التي تساعد على تطبيق المبادئ والقواعد والتوجيهات لتقنية المعلومات، بحيث تمكّن الجهة من تحقيق أهدافها التشغيلية والإستراتيجية.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-06	اعتماد وتعميم وتنفيذ سياسات وإجراءات تقنية المعلومات متضمنة بحد أدنى ما يلي: • الأهداف والنطاق والتطبيق. • المسؤوليات العامة والخاصة لتقنية المعلومات. • الربط بالضوابط التشريعية والتنظيمية الوطنية ذات العلاقة.
5-108-07	وضع سياسة تقنية المعلومات الرئيسة بالمواءمة مع السياسات الأخرى داخل الجهة الحكومية، بحد أدنى ما يلي: • سياسة الأمن السيبراني. • سياسة المخاطر وسياسة استمرارية الأعمال. • سياسة الموارد البشرية.
5-108-08	تحديث سياسات وإجراءات تقنية المعلومات بشكل دوري (سنويًّا على الأقل، أو عند حدوث تغيير جوهري في أهداف السياسة أو الإجراءات المتبعة).

7.1.3 ضوابط تحديد الأدوار والمسؤوليات		
الهدف	تحديد أدوار أصحاب الصلاحية ومسؤولياتهم بحوكمة تقنية المعلومات وإدارتها، والتأكد من أن الأطراف جميعها جميعها في عمليات حوكمة تقنية المعلومات وتشغيلها في الجهة لديهم وعي كامل بالأدوار والمسؤوليات.	
يجب على الجهات الحكومية أن تلتزم بما يلي:		
رقم الضابط		
5-108-09	تكليف المسؤول الأول للوحدة الإدارية المسؤولة عن تقنية المعلومات بإعداد مهام الوحدة الإدارية المسؤول عنها، على أن تشمل، بحد أدنى، ما يلي:	
	5-108-09.01	وضع وتنفيذ استراتيجية وميزانية تقنية المعلومات.
	5-108-09.02	وضع منهجية حوكمة عمليات تقنية المعلومات بناءً على منهجية التحول الرقمي لدى الجهة، واعتمادها من ذوي العلاقة.
	5-108-09.03	تطوير المسؤوليات المتعلقة بممارسات حوكمة تقنية المعلومات وإدارتها.
	5-108-09.04	اعتماد جميع الأوصاف الوظيفية لمنسوبي إدارة تقنية المعلومات.
	5-108-09.05	تصميم واعتماد مؤشرات قياس الأداء، ومؤشرات قياس المخاطر الرئيسة لتقنية المعلومات، بالتنسيق مع الجهات المعنية.
	5-108-09.06	تحديد آلية متابعة الامتثال للوائح والسياسات والضوابط التنظيمية، والإجراءات المتعلقة بتقنية المعلومات.
	5-108-09.07	تحديد ومتابعة وإعداد تقارير مؤشرات قياس الأداء الرئيسية لتقنية المعلومات، بالإضافة إلى مراقبة مؤشرات المخاطر الرئيسية.
	5-108-09.08	تحديد آلية متابعة ومراجعة إبلاغ اللجنة التوجيهية لتقنية المعلومات وهيئة الحكومة الرقمية بحوادث تقنية المعلومات بصورة مستمر.
	5-108-09.09	تحديد آلية للإشراف على التحقيق في الحوادث الرقمية والتقنية المتعلقة بتقنية المعلومات داخل الجهة.
	5-108-09.10	وضع آلية للتأكد من أن جميع منسوبي الجهة ممتثلون للسياسات، والضوابط التنظيمية، وإجراءات العمل لتقنية المعلومات ذات الصلة.

7.1.4 ضوابط إدارة مخاطر تقنية المعلومات	
الهدف	تنفيذ عمليات إدارة مخاطر تقنية المعلومات، ومواءمتها مع إدارة المخاطر المؤسسية بالجهة متضمنة تعريف، وتحليل، ومعالجة، ومراقبة، ومراجعة مخاطر تقنية المعلومات لدى الجهة الحكومية، ووفقاً لما تصدره الهيئة من وثائق تنظيمية ذات صلة.

يجب على الجهات الحكومية أن تلتزم بما يلي:

رقم الضابط		
5-108-10		اعتماد، وتعميم، وتنفيذ سياسات وإجراءات إدارة مخاطر تقنية المعلومات.
5-108-11		مواءمة سياسات وإجراءات إدارة مخاطر تقنية المعلومات مع الضوابط الصادرة لإدارة المخاطر واستمرارية الأعمال للحكومة الرقمية والتنظيمات ذات الصلة.
5-108-12		تضمين إجراءات إدارة مخاطر تقنية المعلومات بما يتسق مع إدارة المخاطر لدى الجهة، وتشمل بحدّ أدنى:
	5-108-12.01	تعريف وتحليل وتصنيف ومعالجة المخاطر.
	5-108-12.02	آلية الإبلاغ وتصعيد المخاطر.
	5-108-12.03	رصد ومراقبة المخاطر، وتحديد خصائصها، وتقديم التقارير الدورية.
5-108-13		تضمين عملية إدارة مخاطر تقنية المعلومات، وسجل الأصول المعلوماتية الرقمية وغير الرقمية الخاصة بالجهة، والمخاطر المرتبطة بها،والذي يشمل بحدّ أدنى:
	5-108-13.01	إجراءات الأعمال والبيانات ذات الصلة.
	5-108-13.02	تطبيقات الأعمال.
	5-108-13.03	مكونات البنية التحتية.
	5-108-13.04	بيانات العلاقات مع الجهات الخارجية المقدمة لخدمات تقنية المعلومات.
5-108-14		القيام بتنفيذ عمليات تقييم مخاطر تقنية المعلومات خلال المراحل التالية وتشمل كحد أدنى: • عند البدء في تنفيذ البرامج والمشاريع التقنية والخدمات الرقمية. • قبل تنفيذ تغييرات حرجة وجذرية في أصول المعلومات والبنية التحتية المعلوماتية. • عند التخطيط للاستعانة بمصادر خارجية، أو خدمات الاستضافة. • قبل شراء أنظمة وأدوات وتقنيات ناشئة جديدة.
5-108-15		تنفيذ تقييم دوري لأصول المعلومات الحالية لتقييم المخاطر بناءً على أهميتها والتهديدات والمخاطر، وتشمل كحد أدنى: • تقييم جميع أصول المعلومات الحرجة مرتين في السنة على الأقل. • تقييم أصول المعلومات غير الحرجة بناء على أهميتها للجهة بشكل دوري (سنويًّا على الأقل).

5-108-16	تنفيذ أنشطة تقييم مخاطر تقنية المعلومات من (ملّاك المخاطر)، بشكل دوري (سنويًّا على الأقل)، على أن يشمل التقييم، بحد أدنى ما يلي: • ملّاك الأعمال والمستفيدين. • رؤساء إدارات تقنية المعلومات. • مسؤولي الأنظمة والتقنيات. • مختصي مخاطر الأمن السيبراني.
5-108-17	تطوير وتنفيذ إستراتيجيات الاستجابة لمخاطر تقنية المعلومات (تجنب، أو تقليل، أو نقل، أو قبول) وإستراتيجيات الرقابة التي تتوافق مع قيم أصول المعلومات ومقدار تحمل المخاطر المعرّفة بالجهة.
5-108-18	اعتماد وتنفيذ مؤشرات المخاطر الرئيسية لتقنية المعلومات KRIs.
5-108-19	قياس فاعلية إجراءات إدارة مخاطر تقنية المعلومات وتقييمها بشكل دوري (سنويًّا على الأقل).

7.1.5 ضوابط إدارة الكفاءات والقدرات لتقنية المعلومات	
الهدف	تزويد منسوبي الجهات الحكومية بالمهارات والمعلومات اللازمة للتعامل مع الأصول الرقمية المختلفة الخاصة بالجهة، وبطريقة خاضعة للرقابة، وتوفير التدريب المناسب لتحديد الضوابط ذات الصلة بتقنية المعلومات وتشغيلها وتطبيقها بكفاءة وفاعلية.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-20	تحديد وتعريف الأدوار داخل قطاع/ إدارة تقنية المعلومات (مثل: المسؤول الأول في الإدارة، ومسؤول قواعد البيانات ومسؤول النظام، ومسؤول الشبكات، ومسؤول المنصات ...إلخ) بالتنسيق مع إدارة الموارد البشرية، ووفق الأنظمة والتعليمات ذات العلاقة.
5-108-21	تطوير الإجراءات لتطبيق فاعلية التعاقب الوظيفي للأدوار الحساسة في الإدارة، ولضمان استمرارية الأعمال.
5-108-22	تقييم المتطلبات والاحتياجات من الكوادر البشرية والأدوار الوظيفية بشكل دوري (سنويًّا على الأقل)، أو بناءً على التغييرات الرئيسة في بيئة العمل.
5-108-23	بالمواءمة مع قرار مجلس الوزراء رقم (555) وتاريخ 1440/09/23هـ، الصادر بالموافقة على ضوابط استخدام تقنيات المعلومات والاتصالات في الجهات الحكومية، يجب وضع خطة تدريب سنوية بالتنسيق مع الموارد البشرية لموظفي تقنية المعلومات، وتنفيذها بالشكل المناسب بناءً على دراسة تحليلية للكفاءات والقدرات، ومراجعة الخطة بشكل دوري (سنويًّا على الأقل) على أن تتضمن بحد أدنى: الموظفين المشاركين في أداء مناصب تقنية المعلومات الحساسة، وتحديد الشهادات المهنية المطلوبة / عملية تقييم المخاطر لتقنية المعلومات / تطوير أو إدارة الأصول المعلوماتية.

7.2 تخطيط تقنية المعلومات

7.2.1 ضوابط تطوير إستراتيجية تقنية المعلومات		
الهدف	تطوير إستراتيجية تقنية المعلومات بما يتواءم مع الأهداف الإستراتيجية للجهة الحكومية.	
يجب على الجهات الحكومية أن تلتزم بما يلي:		
رقم الضابط		
5-108-24	تطوير واعتماد وتنفيذ إستراتيجية تقنية المعلومات، لتتضمن بحد أدنى ما يلي:	
	5-108-24.01	مستهدفات وخطط الحوسبة السحابية للجهات الحكومية الصادر عن هيئة الحكومة الرقمية.
	5-108-24.02	بيئة الأعمال ومكونات تقنية المعلومات الحالية والتوجه المستقبلي، والمبادرات المطلوبة لتحقيق الوضع المستهدف بما يتواءم مع إستراتيجية التحول الرقمي.
	5-108-24.03	تحديد المخاطر التقنية والرقمية الإستراتيجية التي قد يكون لها تأثير على تحقيق أهداف الجهة والحكومة الرقمية، ومدى تأثير تقنية المعلومات وفوائدها العائدة في أهداف الجهة.
5-108-25	وضع خارطة طريق مبادرات تقنية المعلومات لتتضمن ما يلي:	
	5-108-25.01	التقنيات الرقمية المتقدمة لتحسين الإجراءات وطريقة تقديم الخدمات للمستفيدين.
	5-108-25.02	تحديد أولويات تنفيذ المشاريع التقنية المختلفة بناءً على تقييم النتائج والتبعيات الخاصة بها من الإدارات ذات العلاقة.

7.2.2 ضوابط إدارة البنية التقنية	
الهدف	دعم تسريع التحول الرقمي، ورفع مستوى نضج البنية التقنية في الحكومة الرقمية عن طريق المواءمة مع التوجهات الإستراتيجية للجهة وإستراتيجية التحول الرقمي، وإجراءات الأعمال وتقنية المعلومات (المنصات، والتطبيقات، والبيانات، والبنية التحتية للتقنية)؛ لتحقيق الأهداف الإستراتيجية للجهة الحكومية، عن طريق تطبيق الممارسات والمعايير والمنهجيات ذات العلاقة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-26	تطوير إستراتيجية البنية التقنية بما يتواءم مع المنهجية الوطنية للبنية المؤسسية (NORA)، وما يصدر عن الهيئة بهذا الخصوص، على أن تشمل بحد أدنى ما يلي:
5-108-26.01	مخططاً إستراتيجياً للقدرات التقنية للجهة الحكومية وخطط إدارة البنية التقنية واستمرارية الأعمال ومراجعتها بشكل دوري (سنويًّا على الأقل).
5-108-26.02	تنفيذ وتشغيل البنية التقنية الداخلية للجهة.
5-108-26.03	تحديد الفجوات بين الوضع الحالي والمستهدف للبنية التقنية، وتطوير خارطة طريق للتحول الرقمي لتنفيذ المبادرات والمشاريع، ومتابعة حالة التنفيذ مع الأخذ في الحسبان منظور الأعمال، وتوظيف وتطبيق التقنيات الناشئة والمتطلبات التنظيمية.
5-108-27	وضع آلية لمتابعة الامتثال بالتنظيمات والتشريعات ذات العلاقة والالتزام بها.
5-108-28	متابعة مؤشرات الأداء وعمليات الحوكمة لإستراتيجية البنية التقنية، عن طريق تقديم تقارير دورية للإدارة العليا.
5-108-29	مراجعة إستراتيجية البنية التقنية بشكل دوري (سنويًّا على الأقل).

7.2.3 ضوابط إدارة اتفاقيات مستوى الخدمة	
الهدف	وضع الاتفاقيات الرسمية التي تحتوي على الأحكام والشروط التعاقدية لمستوى تقديم الخدمات الرقمية والتقنية، التي توضح أدوار أصحاب المصلحة الداخليين والخارجيين وعلاقاتهم، وضمان مسؤولياتهم وامتثالهم، وقياس الأداء.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-30	تحديد اتفاقيات مستوى الخدمة الداخلي (التشغيلي) لتقنية المعلومات، للاعتماد والتعميم، وللتأكد من فاعليتها لدى الجهة.
5-108-31	أن تتضمن اتفاقية مستوى الخدمة الداخلي (التشغيلي) لتقنية المعلومات كحد أدنى: • أهداف محددة وقابلة لقياس مستوى خدمات تقنية المعلومات، بما يتناسب مع مؤشرات الأداء الرئيسة لدى الجهة وتقييمها بشكل دوري (سنويًّا على الأقل). • أدوار ومسؤوليات المعنيين بين إدارة تقنية المعلومات والإدارات الأخرى داخل الجهة.
5-108-32	تعريف اتفاقيات مستوى الخدمة وتوقيعها مع الأطراف الخارجيين ومزودي الخدمات الرقمية والتقنية للجهة.
5-108-33	أن يكون جميع مقدمي خدمات الإسناد ممتثلين للتشريعات واللوائح ذات الصلة من هيئة الحكومة الرقمية والضوابط الأساسية للهيئة الوطنية للأمن السيبراني، وما يستجد من التشريعات والتنظيمات والضوابط ذات الصلة بحوكمة وإدارة تقنية المعلومات.
5-108-34	توقيع اتفاقيات عدم الإفصاح للمحافظة على سرية البيانات والمعلومات، وحمايتها من مقدمي خدمات الإسناد للجهة.
5-108-35	إعداد نموذج الفحص النافي للجهالة بالتنسيق مع الإدارات ذات الصلة داخل الجهة وتوقيعه من الشركات المزمع التعاقد معها -بشكل مباشر أو غير مباشر- لتقديم خدمات تقنية المعلومات وتحديث بيانات النموذج بشكل سنوي على الأقل، على أن يحتوي النموذج على العناصر التالية بحد أدنى: • **البيانات التعريفية بالشركة:** ○ اسم الشركة. ○ رقم السجل التجاري (تاريخ الإصدار والانتهاء). ○ رقم الترخيص (إن وجد). ○ الكيان القانوني (شركة مساهمة، محدودة، ...). ○ دولة المنشأ. ○ الموقع الجغرافي الرئيسي للشركة. • **الهيكل الإداري والملكية:** ○ أسماء أعضاء مجلس الإدارة وجنسياتهم. ○ قائمة الشركات الأخرى المملوكة للشركة ودولة منشأها -إن وجد-. • **بيانات الاتصال:** ○ رقم هاتف الشركة. ○ اسم ومنصب المسؤول الأول. ○ الموقع الإلكتروني للجهة.

5-108-36	وضع الإجراءات التي توضح العلاقة مع الأطراف الخارجية المقدمة للخدمات الرقمية والتقنية، واعتمادها، وتعميمها، وتنفيذها ويشمل ذلك:	
	5-108-36.01	إجراءات تضمن توافر وحماية البيانات والخدمات الرقمية والتطبيقات التي يتم إسنادها.
	5-108-36.02	إجراءات تتضمن الإبلاغ بالتغييرات في تقديم الخدمات أو التغيير في بنود العقد.
	5-108-36.03	إجراءات تنفيذ تقييم المخاطر كجزء من عملية التعاقد.
	5-108-36.04	إجراءات التصعيد في حالة عدم الالتزام باتفاقية مستوى الخدمة.
	5-108-36.05	إجراءات إنهاء العقد أو فسخه أو تجديده وفق الأنظمة ذات العلاقة.
	5-108-36.06	إصدار التقارير الدورية من مقدمي الخدمات.
5-108-37	أن يكون هناك تعهد من مقدمي الخدمات بتوفير مسؤول ذي خبرة في موقع العمل؛ لتوفير الدعم الفني والتقني المطلوب عند مواجهة أوضاع حرجة للعمليات التشغيلية المسندة.	
5-108-38	يجب مراقبة فاعلية اتفاقيات مستوى الخدمة الداخلي (التشغيلي) لتقنية المعلومات وقياسها وتقييمها بشكل دوري (سنويًّا على الأقل).	
5-108-39	ضمان تنفيذ المراجعة والتدقيق بشكل دوري من الجهة؛ لضمان فاعلية بيئة الضوابط الداخلية لمقدمي خدمات الإسناد.	

7.3 بناء وتطوير وتنفيذ أنظمة تقنية المعلومات

7.3.1 ضوابط اقتناء النظم والتطبيقات	
الهدف	بناء وتطوير وتنفيذ الخدمات الرقمية تتم عن طريق إدارة التغيير، وهي عملية تحديد وتصميم واختبار وتنفيذ التغييرات المتعلقة بالأصول والخدمات الرقمية على التطبيقات، والبرامج، والبيانات، والمنصات.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-40	تحديد إجراءات اقتناء النظم والتطبيقات والخدمات الرقمية، واعتمادها، وتعميمها، وتنفيذها بما يتواءم مع المنهجية الوطنية للبنية المؤسسية.
5-108-41	تحديد متطلبات الأعمال والمتطلبات التقنية والأمنية للنظم والتطبيقات والخدمات الرقمية، واعتمادها كجزء من إجراءات اقتناء النظام.
5-108-42	تنفيذ إجراء دراسة جدوى لمتطلبات الأعمال والتقنية؛ لقياس المنفعة المكتسبة والعائد على الاستثمار في عملية اقتناء النظام أو التطبيق.

5-108-43	تضمين عملية تقييم النظام أو التطبيق، وقدرات الموردين أثناء عملية الاختيار، والمواءمة مع إدارة المشاريع في الجهة، لتشتمل على الأقسام التالية كحد أدنى: • توافق إمكانيات النظام أو التطبيق مع متطلبات الجهة. • خطة مفصلة لمراحل تنفيذ المتطلبات، وتطويرها أو تخصيصها، واختبارها، وبدء التشغيل. • الجدول الزمني لكل مرحلة من مراحل تنفيذ المتطلبات. • الكوادر البشرية والموارد المخصصة لمراحل تنفيذ المتطلبات.
5-108-44	قياس فاعلية إجراءات اقتناء النظم والتطبيقات والخدمات الرقمية، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.3.2 ضوابط متطلبات أمن تقنية المعلومات للتغيير		
الهدف	تحديد متطلبات الهيئة الوطنية للأمن السيبراني، واختبار المتطلبات بدقة لجميع التغييرات التي تُنفّذ في بيئة الاختبار لتقنية المعلومات لدى الجهة، من أجل تحديد الثغرات الأمنية فيها، والتخفيف من حدتها قبل نقلها إلى بيئة التشغيل.	
يجب على الجهات الحكومية أن تلتزم بما يلي:		
رقم الضابط		
5-108-45	استيفاء متطلبات الهيئة الوطنية للأمن السيبراني للتغييرات على الأصول المعلوماتية الرقمية.	
5-108-46	تضمين متطلبات الهيئة الوطنية للأمن السيبراني خلال عملية تحديد المتطلبات في بيئة تقنية المعلومات قبل الانتقال إلى مرحلة التشغيل.	
5-108-47	استيفاء متطلبات الهيئة الوطنية للأمن السيبراني لمشاريع تطوير المنصات والتطبيقات والخدمات الرقمية الخاصة للجهة، ويشمل ذلك:	
	5-108-47.01	استخدام معايير التطوير الآمن للتطبيقات.
	5-108-47.02	استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها.
	5-108-47.03	إجراء الاختبارات المناسبة للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة.
	5-108-47.04	إجراء مراجعة للإعدادات والتحصين وحزم التحديثات قبل الانتقال لمرحلة التشغيل.
5-108-48	إصدار التقارير الدورية التي توضح حالة الامتثال لمتطلبات الهيئة الوطنية للأمن السيبراني.	
5-108-49	مراجعة متطلبات الهيئة الوطنية للأمن السيبراني في بيئة تقنية المعلومات بشكل دوري (سنويًّا على الأقل).	

7.3.3 ضوابط إدارة تهيئة النظم والتطبيقات	
الهدف	تحديد عملية إدارة تهيئة مواصفات النظم والمنصات والتطبيقات، واعتمادها، وتعميمها، وتنفيذها؛ من أجل الحفاظ على معلومات موثوقة ودقيقة حول عناصر التهيئة لأصول المعلومات الرقمية الخاصة بالجهة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-50	إعداد إجراءات إدارة التهيئة والتغيير، واعتمادها، وتعميمها، وتنفيذها داخل الجهة، وتشمل:
	5-108-50.01 الأدوار والمسؤوليات لتنفيذ إدارة التهيئة.
	5-108-50.02 تحديد وتسجيل بنود التهيئة ومدى أهميتها فيما يتعلق بدعمها لعمليات التشغيل.
	5-108-50.03 العلاقات المتبادلة والاعتمادية بين عناصر التهيئة بين مختلف أصول المعلومات.
	5-108-50.04 آلية التحقق الدوري من عناصر التهيئة في بيئة التشغيل لتقنية المعلومات.
5-108-51	إنشاء قاعدة بيانات لإدارة التهيئة؛لتحديد المعلومات المتعلقة بالأصول الرقمية الخاصة بالجهة، والحفاظ عليها، والتحقق منها بشكل دوري.
5-108-52	مراجعة إجراءات وعمليات إدارة التهيئة، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.3.4 ضوابط إدارة التغيير	
الهدف	إنشاء عملية إدارة التغيير؛ لضمان أن التغييرات التي تطرأ على أصول المعلومات الرقمية والمنصات الخاصة بالجهة تُصنّف وتُختبر وتُعتمد قبل تعميمها في بيئة التشغيل.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-53	إعداد إجراءات عملية إدارة التغيير، واعتمادها، وتعميمها، وتنفيذها داخل الجهة، على أن تتضمن الإجراءات بحد أدنى ما يلي: • تعريف متطلبات التغيير وآلية اعتمادها. • تقييم المخاطر والأولوية للتغيير. • اختبار التغيير وخطة التراجع في حالة عدم نجاح تنفيذ التغيير. • أدوار ومسؤوليات عملية التغيير. • عملية إدارة الإصدارات. • توثيق التغيير والدروس المستفادة. • التوعية والتدريب على التغيير.
5-108-54	اعتماد طلب التغيير من اللجنة المعنية أو أصحاب الصلاحية قبل البدء بتنفيذ أي من التغييرات.
5-108-55	تسجيل أحداث أي تغييرات في أصول المعلومات الرقمية، ومراقبتها وتوثيقها بصورة مستمرة.
5-108-56	الفصل بين الاختبارات على بيئة التطوير وبيئة الاختبار وبيئة ما قبل التشغيل، وبيئة التشغيل في جميع حالات طلب التغيير.
5-108-57	مراقبة صلاحيات الدخول إلى بيئات الاختبارات المختلفة؛ لفصل المهام والمسؤوليات قبل النشر على بيئة التشغيل.
5-108-58	توثيق بيانات طلب التغيير والاختبارات، على المعلومات التالية، وتشمل بحدّ أدنى ما يلي:
5-108-58.01	اسم حالة الاختبار، والمعرف الفريد (Test ID).
5-108-58.02	حالة الاختبار التي صممت واختبرت.
5-108-58.03	وصف حالة الاختبار مع تحديد توقعات نتيجة الاختبار.
5-108-58.04	أولوية الاختبار وتاريخ التنفيذ.
5-108-58.05	نوع البيانات المستخدمة للاختبار.
5-108-58.06	شهادة اختبار أمان وفاعلية التغيير في حالة الاستعانة بطرف خارجي لتنفيذ التغيير.
5-108-59	تنفيذ وتوثيق الأنواع التالية من الاختبارات كجزء من إدارة التغيير:
5-108-59.01	اختبارات الأمن السيبراني وأمن المعلومات.
5-108-59.02	اختبار قبول المستخدم من مالك الأعمال.
5-108-59.03	اختبارات المهام - (Functional Test).
5-108-59.04	اختبارات الأداء – (Performance Test).
5-108-60	تنفيذ إجراءات إدارة الإصدارات أثناء مرحلة الاختبار، والنشر على بيئة التشغيل.
5-108-61	أن تكون عملية الإصدارات قد تمت في النظام أو التطبيق المماثل في موقع التعافي من الكوارث، بعد التنفيذ الناجح للتغييرات في بيئة التشغيل في الموقع الرئيس.
5-108-62	مراجعة طلبات التغييرات الطارئة المتعلقة بأصول المعلومات الرقمية والتقنية؛ لأغراض مرجعية أو تدقيقية.

7.3.5 ضوابط تطوير النظم والتطبيقات	
الهدف	حوكمة منهجيات وآليات تطوير النظم والتطبيقات، والخدمات الرقمية والمنصات، واعتمادها، وتنفيذها؛ لضمان تنفيذ متطلبات الحكومة الرقمية، وما يتوافق مع قواعد تنظيم البرمجيات الحكومية الحرة ومفتوحة المصدر الصادرة بقرار مجلس الوزراء رقم (14) بتاريخ 02 /01 /1443هـ.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-63	إعداد منهجية وإجراءات تطوير النظم والتطبيقات والمنصات، واعتمادها، وتعميمها، وتنفيذها، وتقييمها، على أن تتضمن الإجراءات بحد أدنى ما يلي: • وثيقة تصميم النظام أو التطبيق. • منهجية التطوير، مثل: النهج المرن (Agile)، ونهج الشلال (Waterfall) . • معايير كتابة لغات البرمجة الآمنة. • أنواع ونهج الاختبارات مثل: ○ اختبار الوحدات (Unit Test). ○ واختبار الانحدار (Regression Test). ○ واختبار الضغط (Stress Test). • التحكم في الإصدارات وآلية التوثيق. • مراقبة جودة تطوير النظام، وإدارة التصحيحات. • آلية نقل وترحيل البيانات. • تدريب المستفيدين.
5-108-64	تضمين متطلبات التصميم ذات المستوى المفصل (Low Level Design) في وثيقة تصميم النظام، بحد أدنى: • متطلبات التهيئة (Configurations). • متطلبات التكامل (Integration). • متطلبات الأداء. • متطلبات تعريف البيانات.
5-108-65	تضمين ضوابط إدارة المخاطر واستمرارية الأعمال، وضوابط الأمن السيبراني، في عملية تطوير النظام بما يتواءم مع التنظيمات المحلية وأفضل الممارسات الدولية.
5-108-66	تنفيذ مراجعة الكود المصدري لجميع التطبيقات المطورة داخل الجهة، والتأكد من توثيق الكود المصدري لكل إصدار جديد؛ للرجوع له عند الحاجة.

5-108-67	عند وجود اتفاقيات ضمان لبناء البرمجيات، يجب تضمين العناصر التالية بحد أدنى:	
	5-108-67.01	تأمين حقوق غير محدود للشفرة المصدرية؛ لإعادة الاستخدام والنسخ والتعديل والتوزيع بين الجهات الحكومية.
	5-108-67.02	حزم التحديثات والإصدارات بحسب فترات زمنية محددة، أو بحسب التحديثات الحرجة والثغرات الأمنية.
	5-108-67.03	تسليم مزود الخدمة الشفرة المصدرية والمستندات المتعلقة بها إلى الجهة الحكومية ورفعها لمستودع البرمجيات الحكومية والتي تتضمن عند توقف مزود الخدمة عن تقديم خدماته أو إلغاء المشروع.
	5-108-67.04	الغرامات المالية على مزودي الخدمة في حالات عدم الوفاء بالمتطلبات وفق الأنظمة والتعليمات ذات العلاقة.
5-108-68	تقييم جودة جميع التغييرات في الأنظمة والتطبيقات والمنصات قبل نقلها وتطبيقها على بيئة التشغيل من الوحدة الإدارية للجودة الشاملة التي تختص بقياس ومراقبة جودة عمليات تقنية المعلومات.	
5-108-69	إعداد تقارير نتائج التقييم ومراجعة الجودة، ورفعها إلى أصحاب المصلحة المعنيين داخل الجهة؛ لتنفيذ خطط التصحيح المقترحة.	
5-108-70	فحص ومتابعة تنفيذ التصحيحات لجميع الأنظمة والتطبيقات بشكل دوري، والكشف عن أي ثغرات في الأنظمة والخدمات الرقمية.	
5-108-71	مراقبة الأنظمة والتطبيقات بعد تنفيذ التصحيحات على بيئة التشغيل الفعلية؛ للتأكد من عدم وجود أي مشكلة، ودراسة الأسباب الجذرية في حال تحديد مشكلة بعد التنفيذ والعمل على إصلاحها.	
5-108-72	مراقبة فاعلية إجراءات ومنهجية تطوير النظام وتقييمها بشكل دوري (سنويًّا على الأقل).	

7.3.6 ضوابط إدارة الأصول الرقمية والتقنية	
الهدف	توفر رؤية واضحة للجهة لأصول المعلومات الرقمية والتقنية الخاصة بالجهة عن طريق تطوير قائمة جرد يتم تحدث باستمرار لإدارة الأصول بصورة فعّالة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-73	إعداد واعتماد وتعميم وتنفيذ سياسات واجراءات وعمليات إدارة الأصول على أن تتضمن كحد أدني ما يلي: • الإعداد والتشغيل الأولي للأصول الرقمية والتقنية. • تعريف الأصول، وتصنيفها، ووسمها، وطريقة التعامل معها، ومعالجتها. • آلية حصر الأصول والاستخدام الفعلي والعمر الافتراضي. • آلية صلاحيات الإتلاف والموافقات، والتخلص من الأصول الرقمية والتقنية، وبما لا يزيد عن (10)سنوات.
5-108-74	حصر أو جرد لكامل الأصول التقنية والرقمية في سجل، ويتم تحديثه بشكل مستمر (سنوي على الأقل)، أو كلما تم إضافة أصل جديد، أو إتلاف أو إزالة أصل قديم.
5-108-75	إنشاء قائمة بالأصول الرقمية والتقنية الحساسة للجهة، وتحديثها بشكل دوري (سنويًّا على الأقل)، أو كلما تم إضافة أصل جديد، أو إتلاف أو إزالة أصل قديم.
5-108-76	إتخاذ تدابير لمعالجة الأصول الحساسة؛ لضمان استمرارية توافر الخدمات الحيوية والحرجة للجهة (خطط استمرارية الأعمال).
5-108-77	على مراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات، تنفيذ المتطلبات التالية كحد أدنى: • السماح بالوصول المقيد بناءً على الصلاحيات إلى مراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات. • تسجيل دخول الزوار إلى مراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات، ومرافقتهم من قبل شخص مفوض من الجهة، ومراجعة سجل الزوار بشكل دوري. • توفير أنظمة وأدوات الأمن والسلامة، وأنظمة الكشف عن الدخان والحريق. • توفير أنظمة التحكم في الرطوبة، ومراقبة درجة الحرارة. • توفير كاميرات المراقبة (CCTV) داخل وخارج مراكز البيانات والتعافي من كوارث تقنية المعلومات والاتصالات.
5-108-78	التأكد من امتثال مقدمي خدمات الإسناد لمتطلبات هيئة الحكومة الرقمية، والهيئة الوطنية للأمن السيبراني، وهيئة الاتصالات والفضاء والتقنية، والجهات الحكومية ذات العلاقة، عند استضافة مراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات.
5-108-79	ضمان فاعلية الضوابط الرقابية في العقود المبرمة مع مقدمي الخدمات المسند إليهم استضافة مراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات، وذلك من خلال تقديم ما يأتي كحد أدنى: تقارير ضوابط الأنظمة والمنظمة (System and Organization Controls-SOC) من مقدمي خدمات الإسناد للجهة بشكل دوري (سنويًّا على الأقل).
5-108-80	الإتلاف الآمن للأصول الرقمية والتقنية بطريقة خاضعة للرقابة.
5-108-81	مراقبة واختبار الضوابط لمراكز البيانات ومراكز التعافي من كوارث تقنية المعلومات والاتصالات، وتقييمها بشكل مستمر لدى الجهة.
5-108-82	مراقبة فاعلية عملية إدارة الأصول، وقياسها، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.3.7 ضوابط إدارة مشاريع تقنية المعلومات	
الهدف	اتباع منهجية فعالة لإدارة مشاريع تقنية المعلومات والخدمات الرقمية، ومراقبة المخاطر المتعلقة بها طوال مدة العمل على المشروع.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-83	إنشاء إطار لإدارة المشاريع التقنية والرقمية. ويتضمن السياسات والإجراءات المعتمدة لإدارة المشروع من مرحلة البدء بالمشروع حتى مرحلة الإغلاق بالمواءمة مع مكتب المشاريع داخل الجهة الحكومية.
5-108-84	إشراك الإدارة المكلفة بالأمن السيبراني أثناء المراحل المختلفة من دورة حياة إدارة مشاريع تقنية المعلومات.
5-108-85	مراجعة جميع مخرجات المشاريع التقنية والرقمية، قبل بدء التنفيذ في بيئة التشغيل؛لضمان جودة المخرجات، وتحقيق الأهداف.
5-108-86	مراقبة وقياس فاعلية عملية إدارة مشاريع تقنية المعلومات، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.3.8 ضوابط إتاحة الخدمات الرقمية وإدارة القدرات والسعة	
الهدف	التأكد من استمرارية وإتاحة الخدمات الرقمية؛ لدعم أهداف الجهة والحكومة الرقمية، وتجنب بطء أو توقف أداء المنصات والأنظمة، عن طريق مراقبة المؤشرات والحدود القصوى للاستخدام الحالي للمنصات والنظم، والتنبؤ بمستوى الأداء ومتطلبات القدرات والسعة في المستقبل؛ لتجنب تعطل خدمات الجهة، والتأثير على استمرارية أعمال الحكومة الرقمية.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-87	إنشاء إجراءات إتاحة الخدمات الرقمية وإدارة القدرات والسعة، واعتمادها، وتعميمها، وتنفيذها.
5-108-88	بناء خطة إدارة القدرات والسعة لإتاحة الخدمات الرقمية، على أن تحتوي بحد أدنى العناصر التالية: • القدرة والسعة الحالية للنظم، والموارد، والأصول الرقمية، والتقنية. • المواءمة مع الأهداف التشغيلية للجهة الحالية والمستقبلية. • متطلبات خطط الاستمرارية والإتاحة (يشمل ذلك حالات البطء أو التوقف في قنوات خدمة المستفيدين والخدمات الرقمية). • تحديد الأدوار والمسؤوليات للحفاظ على الخطة. • تحديد الاعتمادية على مقدمي الخدمات كجزء من تخطيط القدرات والسعة ضمن خطط استمرارية الأعمال.
5-108-89	إعداد ومراقبة مؤشرات أداء الخدمات الرقمية والنظم، وتتضمن العناصر التالية، كحد أدنى:
5-108-89.01	اتفاقية مستوى الخدمة المتفق عليها مع الأطراف الخارجية.
5-108-89.02	البنية التحتية لتقنية المعلومات.
5-108-89.03	البطء والتوقف في الخدمات الرقمية والأنظمة الأساسية التي تدعم قنوات خدمة المستفيدين.
5-108-90	توثيق ومتابعة وتقديم التقارير ونتائج مؤشرات الأداء إلى الإدارة العليا واللجنة التوجيهية بشكل دوري.
5-108-91	مراقبة فاعلية إجراءات استمرارية وإتاحة الخدمات الرقمية والنظم لإدارة القدرات والسعة، وقياسها، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.4 تحقيق القيم المضافة من تقنية المعلومات

7.4.1 ضوابط إدارة خدمات النسخ الاحتياطي وحماية البيانات	
الهدف	إتاحة الخدمات الرقمية المقدمة من الجهة للمستفيدين، عن طريق تنفيذ إستراتيجيات وسياسات وإجراءات لإدارة عمليات النسخ الاحتياطي للبيانات والاستعادة والاختبار، وتنفيذها بشكل فعال؛ لضمان استرداد البيانات والخدمات لدى الجهة في الوقت المستهدف.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-92	وضع سياسات وإجراءات إدارة النسخ الاحتياطي، واستردادها للبيانات، واعتمادها، وتعميمها، وتنفيذها، بما لا يتعارض مع ما جاء في التنظيمات ذات الصلة والصادرة من الجهات ذات العلاقة.
5-108-93	تشمل سياسات إدارة النسخ الاحتياطي للبيانات ما يلي، بحد أدنى: • المواءمة مع سياسات استمرارية الأعمال. • آلية تنفيذ النسخ الاحتياطي والاسترداد. • آلية بديلة للنسخ الاحتياطي والاسترداد. • آلية الترميز والتخزين والاسترجاع للبيانات. • الاحتفاظ بالبيانات وفقا للمتطلبات القانونية والتنظيمية والتشريعية المحلية.
5-108-94	تحديد إجراءات النسخ الاحتياطي والاستعادة، واعتمادها، وتنفيذها، وأن تشمل على العناصر التالية كحد أدنى: • متطلبات حفظ البيانات بما يتواءم مع أهداف خطط استمرارية الأعمال المعتمدة. • منهجية النسخ الاحتياطية مثل: (غير متصل بالإنترنت، عبر الإنترنت، كامل، تدريجي). • جدول إجراء النسخ الاحتياطي مثل: (يوميًا، أسبوعيًا، شهريًا، نصف سنوي، سنويًا).
5-108-95	تزامن البيانات والمعلومات بين مركز البيانات وموقع التعافي من كوارث تقنية المعلومات والاتصالات طبقًا لمتطلبات إستراتيجية إدارة النسخ الاحتياطي وخطط استمرارية الأعمال.
5-108-96	اختبار خطط التعافي من كوارث تقنية المعلومات والاتصالات، واختبار دوري لقدرة النسخ الاحتياطي؛ لتقليل احتماليات انقطاع الخدمات الرقمية في حالة وقوع كارثة.
5-108-97	تشفير جميع وسائط النسخ الاحتياطي التي تحتوي على معلومات حرجة وحيوية أو سرية قبل النقل إلى خارج الموقع بهدف التخزين الآمن، وذلك بما لا يتعارض مع الأنظمة والتنظيمات ذات العلاقة.
5-108-98	قياس فاعلية إجراءات النسخ الاحتياطي والاستعادة، وتقييمها بشكل دوري (سنويًا على الأقل).

7.4.2 ضوابط الاعتمادية والترابط	
الهدف	إدارة أوجه الاعتمادية والترابط المتعلقة بأصول المعلومات الرقمية والتقنية الحرجة للجهة؛ لضمان توافر واستمرارية عمليات الجهة للخدمات الرقمية للمستفيدين والأعمال التشغيلية.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-99	تحديد وتنفيذ إجراءات الاعتمادية وترابط الأصول الرقمية والتقنية لدى الجهة، واعتمادها، وتعميمها، وتنفيذها.
5-108-100	تحديد أوجه الاعتمادية والترابط بين أصول المعلومات الرقمية والمنصات والعمليات الحرجة داخل بنيتها التحتية، وتضمينها كجزء من اختبار خطة استمرارية الأعمال والتعافي من كوارث تقنية المعلومات والاتصالات.
5-108-101	تحديد أصحاب المصلحة والمستفيدين المعنيين الداخليين والخارجيين، وأهميتهم للمنصات والخدمات الرقمية، وتحديث بياناتهم سنويًّا على الأقل.

7.4.3 ضوابط بنية الشبكة المعلوماتية ومراقبتها	
الهدف	إدارة ومراقبة الشبكة المعلوماتية والرقمية للجهة عن طريق تنفيذ ضوابط للحد من الأحداث التقنية غير المصرح بها على الشبكة المعلوماتية للجهة أو لمنعها.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-102	وضع سياسات وإجراءات الاستخدام المقبول للشبكة المعلوماتية والرقمية للجهة، واعتمادها، وتعميمها، وتنفيذها وفقًا للمتطلبات القانونية والتنظيمية والتشريعية المحلية.
5-108-103	تصميم واعتماد مخطط الشبكة الرقمية الذي يوضح البنية التحتية التقنية الحالية الكاملة للجهة.
5-108-104	توضيح مكونات الشبكة الأمنية، وينبغي وضع متطلبات أمنية للوصول إلى تلك المكونات؛ لضمان السماح بالمرور المصرح به فقط.
5-108-105	عزل الشبكة التقنية والرقمية للزوار، وفصلها عن الشبكة الداخلية بشكل آمن.
5-108-106	التأكد من أن الوصول عن بُعد للشبكة المعلوماتية للجهة مقتصر فقط على مجموعة محددة من عناوين الشبكة المعرفة، ومراقبتها بشكل مستمر.
5-108-107	ضمان إجراء مراقبة على جميع مكونات الشبكة الحرجة والحساسة بشكل مستمر.
5-108-108	قياس فاعلية الاستخدام المقبول للشبكة المعلوماتية والرقمية، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.4.4 ضوابط البرمجيات الافتراضية	
الهدف	تنفيذ آلية لإنشاء برامج المساعدة الافتراضية، والحاويات التقنية الافتراضية، وتشغيلها، وتخزينها، واستخدامها، والتخلص منها عند انتهاء الحاجة إليها بطريقة آمنة وفعالة للجهة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-109	تطوير إجراءات إعداد بيئة التشغيل التقنية الافتراضية، وتعميمها، وإعتمادها، والتأكد من تنفيذهابصورة آمنة.
5-108-110	التأكد من مواءمة السياسات والإجراءات والمعايير المحددة من الجهة مع التشريعات والتنظيمات المحلية ذات الصلة.
5-108-111	التأكد من تطبيق جميع الضوابط الأمنية على المكونات الافتراضية المنفذة بنفس مستوى الأنظمة ومكونات الشبكة المادية.
5-108-112	تنفيذ ضوابط التحقق من الهوية الشبكية الممتثلة لضوابط الهيئة الوطنية للأمن السيبراني.
5-108-113	تفعيل سجل الأحداث الرقمي لمراجعة ومراقبة جميع التغييرات على بيئة التشغيل والمكونات الافتراضية، التي يجب أن تتضمن: • أحداث الإنشاء والنشر والإزالة. • جميع الأنشطة ذات الامتيازات العالية والأنشطة ذات الصلاحيات النافذة.
5-108-114	قياس فاعلية عملية تشغيل بيئة التقنية الافتراضية،وتقييمها بشكل دوري (سنويًا على الأقل).

7.4.5 ضوابط معالجة حزم البيانات	
الهدف	تحديد سياسات وإجراءات إدارة حزم البيانات، واعتمادها، وتنفيذها من أجل إدارة معالجة البيانات وحزم العمليات، أو أتمتة العمليات بشكل دفعات لمعالجة البيانات، بطريقة فعالة وخاضعة للرقابة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-115	إصدار سياسات وإجراءات معالجة حزم البيانات، واعتمادها، وتنفيذها.
5-108-116	تتضمن إجراءات معالجة حزم البيانات الأقسام التالية، بحد أدنى: • جدولة تنفيذ العمليات بحسب (اليوم، الأسبوع، الشهر، السنة). • الأدوار والمسؤوليات. • رقابة الحزم أو الدفعات لتدفق العمليات. • معالجة الأخطاء أو الاستثناءات. • آلية التبليغ والتصعيد.
5-108-117	اعتماد التغييرات في جداول الحزم والدفعات من ذوي العلاقة.
5-108-118	الاحتفاظ بسجل الأحداث الذي يحتوي على معلومات حول حالة تنفيذ حزم العمليات والدفعات، مثل:(ناجحة أو غير ناجحة).
5-108-119	قياس فاعلية عملية إدارة معالجة حزم البيانات، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.5 مراقبة الأداء والتحسين المستمر

7.5.1 ضوابط إدارة الأداء	
الهدف	تحقيق أهداف الخدمات الرقمية والتقنية المقدمة من الجهة عن طريق قياس كفاءة وفاعلية عمليات تقنية المعلومات بشكل مستمر، عن طريق مراقبة مؤشرات قياس الأداء الرئيسة، ومؤشرات الأهداف، والنتائج الرئيسة.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-120	تطوير واعتماد وتنفيذ وتعميم مؤشرات قياس الأداء الرئيسة، لقياس مدى جودة تنفيذ عمليات تقنية المعلومات وأداء المنصات والخدمات الرقمية لدى الجهة.
5-108-121	تضمين المستويات التالية في مؤشرات قياس الأداء الرئيسة: • حوكمة تقنية المعلومات. • الكوادر البشرية. • العمليات والخدمات الرقمية. • الحلول التقنية.
5-108-122	متابعة مستوى الأداء، وتقديم تقارير دورية للإدارة العليا بالنتائج.
5-108-123	قياس فاعلية عملية إدارة الأداء، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.5.2 ضوابط التدقيق الداخلي على تقنية المعلومات	
الهدف	قياس كفاءة الضوابط التقنية والرقمية عن طريق التنفيذ المستمر للتدقيق الداخلي لتقنية المعلومات على التطبيقات والخدمات الرقمية والمنصات، ووفقًا للضوابط التنظيمية، واتباع المنهجيات ذات الصلة والأدوات المستخدمة محليًّا ودوليًّا، للتحقق من الضوابط المطبقة في الجهة وتصميمها.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-124	تطوير خطة للتدقيق على تقنية المعلومات، مع تحديد النطاقات الرئيسة، والتي تشمل (حوكمة تقنية المعلومات، والكوادر البشرية، والعمليات والتقنيات).
5-108-125	مواءمة تدقيق تقنية المعلومات مع ضوابط تدقيق الأمن السيبراني، وتوثيق النتائج، وعرضها على أصحاب الصلاحية.
5-108-126	اعتماد دورية التدقيق على ضوابط تقنية المعلومات بشكل منتظم (سنويًّا على الأقل).
5-108-127	مواءمة دورة التدقيق الداخلي على تقنية المعلومات، مع درجة حساسية ومخاطر أنظمة أو إجراءات تقنية المعلومات.
5-108-128	اعتماد خطة تدقيق على تقنية المعلومات من اللجنة التوجيهية في الجهة، ورفع التقارير إلى اللجنة بشكل دوري.
5-108-129	إصدار تقرير تدقيق على تقنية المعلومات، على أن يحتوي على ما يلي، كحد أدنى: • الملاحظات والتوصيات وخطط التصحيح أثناء فترة زمنية محددة. • تحديد مسؤولية تنفيذ خطط التصحيح.
5-108-130	إعداد إجراءات لمتابعة خطط العلاج لتتمكن الجهة من تتبع ومراقبة حالة التنفيذ.
5-108-131	تنفيذ عمليات التدقيق الدوري على الالتزام بضوابط حوكمة تقنية المعلومات من طرف مستقل.
5-108-132	قياس فاعلية الخطة المعتمدة للتدقيق الداخلي على تقنية المعلومات، وتقييمها بشكل دوري (سنويًّا على الأقل).

7.5.3 ضوابط الامتثال	
الهدف	فاعلية الامتثال للتنظيمات والتشريعات ذات الصلة بتقنية المعلومات والخدمات الرقمية والمنصات، عن طريق وضع آليات تساعد على تحديد مستوى الامتثال، والإبلاغ، والتصعيد لذوي العلاقة داخل الجهة وخارجها.
يجب على الجهات الحكومية أن تلتزم بما يلي:	
رقم الضابط	
5-108-133	وضع سياسات وإجراءات الامتثال للضوابط التنظيمية والمتطلبات المتعلقة بتقنية المعلومات على أن تتضمن ما يلي: • التنفيذ الدوري (سنويًّا على الأقل)، ووضع الخطط التصحيحية، أو عند صدور متطلبات تنظيمية جديدة يتطلب الامتثال لها. • آلية إشراك ذوي العلاقة وأصحاب المصلحة. • آلية الاحتفاظ بسجل محدث لجميع المتطلبات التشريعية، والتنظيمية، والتعاقدية ذات الصلة وتأثيرها، والإجراءات الداخلية المطلوبة لتسيير العمليات التشغيلية المعتمدة على تقنية المعلومات.
5-108-134	رفع تقارير دورية بقياس الامتثال للمسؤول الأول في الجهة واللجنة التوجيهية لتقنية المعلومات، ومتابعة الخطط التصحيحية،بحسب ما تراه الجهة.

8. جدول التعريفات

يُقصد بالألفاظ والعبارات الآتية- أينما وردت في هذه الوثيقة- المعاني المُبيّنة أمام كلٍّ منها، ما لم يقتض السياق خلاف ذلك:

المصطلح	التعريف
الهيئة	هيئة الحكومة الرقمية.
الحكومة الرقمية	دعم العمليات الإدارية والتنظيمية والتشغيلية داخل القطاعات الحكومية – وفيما بينها – لتحقيق التحول الرقمي، وتطوير وتحسين وتمكين الوصول بسهولة وفاعلية للمعلومات والخدمات الحكومية.
الجهات الحكومية	الوزارات والهيئات والمؤسسات العامة والمجالس والمراكز الوطنية، وما في حكمها.
الضوابط	الاشتراطات التي يجب على الجهات الحكومية أن تمتثل لها، والتي يجب عليها القيام بها لتحقيق ما ورد في السياسة المرتبطة بها من مستهدفات وأحكام عامة.
الإدارة العليا	جميع المسؤولين عن اتخاذ القرارات داخل الجهة.
أصحاب المصلحة	الأطراف والجهات التي تؤثر وتتأثر بقرارات وتوجهات وإجراءات وأهداف وسياسات ومبادرات الحكومة الرقمية، وتشاركها بعضًا من اهتماماتها ومخرجاتها، وتتأثر بأي تغير يحدث بها.
التحول الرقمي	تحويل نماذج الأعمال وتطويرها بشكل استراتيجي، لتكون نماذج رقمية مستندة على بيانات وتقنيات وشبكات الاتصالات.
استراتيجية تقنية المعلومات	خطة تحدد كيفية استخدام تقنية المعلومات لتحقيق أهداف الأعمال والتحول الرقمي في الجهة، وتشمل (تحليل الوضع الحالي والمستقبلي لتقنية المعلومات، وتحديد الفرص والتحديات والأولويات، ووضع الرؤية والرسالة والأهداف والمؤشرات لتقنية المعلومات، وتصميم البرامج والمشاريع والخدمات والأنظمة التي تدعم تقنية المعلومات، وتوزيع الموارد والمسؤوليات والصلاحيات لتنفيذ الاستراتيجية، وتقييم الأداء).
إطار تقنية المعلومات	تحويل نماذج الأعمال وتطويرها بشكل استراتيجي، لتكون نماذج رقمية مستندة على بيانات وتقنيات وشبكات الاتصالات.
البنية التحتية لتقنية المعلومات	مجموعة من مكونات تقنية المعلومات التي تشكّل أساس خدمة تقنية المعلومات، وتشمل عادة المكونات المادية (جميع أجهزة النقاط الطرفية، والخوادم، وأجهزة ومرافق الشبكات)، بالإضافة إلى مختلف مكونات البرامج والشبكات.
اتفاقيات مستوى الخدمة الخارجي	عقود تحدد الشروط والمعايير والمسؤوليات بين طرفين لضمان تحسين جودة الخدمات وتقليل المخاطر على الجهة.
اتفاقيات مستوى الخدمة الداخلي (التشغيلي)	عقود تحدد المسؤوليات والمتطلبات والمعايير بين الوحدات أو الأقسام الداخلية في الجهة؛ لضمان التنسيق والتعاون في تقديم الخدمات اللازمة.

الأنشطة ذات الامتيازات	تصنيف نشاط بكونه مستعجلًا من أجل تفادي الآثار غير المقبولة على الأعمال أثناء الانقطاع.
الموارد	تشمل الموارد المالية والمعلومات والمهارات والأفراد والتقنيات التي تحصل عليها الجهة، وتستخدمها لتحقيق أهدافها وغاياتها التنظيمية.
الامتثال	مدى استيفاء الجهة للمتطلبات الإلزامية.
حالات عدم الالتزام	عدم استيفاء أحد المتطلبات.
التحسين المستمر	نشاط متكرر لتعزيز أداء عمل تقنية المعلومات في القطاع الحكومي.
المخاطر	احتمالية وقوع حدث يترتب عليه آثار سلبية أو إيجابية
إدارة المخاطر	تطبيق الاستراتيجيات والسياسات والإجراءات لمنع نشوء مخاطر جديدة، والحد من المخاطر القائمة، وإدارة المخاطر المتبقية، من خلال توقع الأخطار، وتحديدها، وتحليل المخاطر، وتقييمها، وتحديد أولوياتها، ومراقبتها، ومراجعتها، والوقاية والتخفيف من الآثار السلبية الناجمة عنها.
مؤشرات المخاطر الرئيسية	مقياس يُستخدم لمراقبة التغيرات في مستوى التعرض للخطر، ويُستخدم كأحد وسائل الإنذار المبكر للمخاطر.
سجل المخاطر	وثيقة تحتوي على قائمة المخاطر، وتتضمن جميع البيانات والمعلومات عنها، ومنها: تاريخ تسجيل الخطر، رمز الخطر، عنوان الخطر، القطاع، مالك الخطر، تصنيف الخطر، وصف الخطر، سيناريو وقوع الخطر، مستوى الاحتمالية، مستوى التأثير، مستوى المخاطر، مستوى الثقة في تقييم الاحتمالية والأثر، المناطق المتأثرة، مؤشرات المخاطر الرئيسية، استراتيجية التخفيف، التدابير الوقائية، مؤشرات التحكم الرئيسية، خطط الاستجابة والتعافي، الجهات المعنية بالاستجابة، الجهات المعنية بالتعافي، جهات الدعم والإسناد.
استمرارية الأعمال	الموارد والإمكانات والقدرات والإجراءات والأعمال اللازمة للاستمرار في تقديم الخدمات الأساسية والمنتجات الضرورية بمستويات محددة مسبقًا، وبإطار زمني مقبول، في حال التعرض للتعطل أو حدوث انقطاع.
خطط استمرارية الأعمال	وثيقة تحدد الإطار العام لإدارة وتنسيق وتوجيه الموارد والإمكانات والقدرات البشرية والفنية والإجراءات، للاستجابة للانقطاع، واستئناف العمليات لتقديم المنتجات الضرورية والخدمات الأساسية، والتعافي في أسرع وقت ممكن لاستمرارية أعمال الجهة.
الانقطاع	حدث متوقع أو غير متوقع يسبب انحرافًا سلبيًّا غير مخطط له عن خطة تسليم المنتجات والخدمات وفق أهداف الجهة.
تحليل أثر انقطاع الأعمال	تحليل عمليات وأنشطة الأعمال ذات الصلة بتقديم الخدمات الأساسية والمنتجات الضرورية، والآثار المترتبة على تعطل أو انقطاع تلك الأعمال.
التعافي من كوارث تقنية المعلومات والاتصالات	قدرة عناصر التعافي من كوارث تقنية المعلومات والاتصالات – ويشمل ذلك جميع التقنيات الرقمية – لدى الجهة على استعادة أنظمتها الحيوية إلى مستوى مقبول خلال فترة زمنية محددة سلفًا بعد حدوث انقطاع.

العملية	مجموعة من الأنشطة المترابطة أو المتفاعلة التي تحوّل المُدخلات إلى مُخرجات.
التدريب	بناء المهارات والكفاءات للرفع من أداء الموظفين فيما يتعلق بأدوار أو مسؤوليات محددة.
تقييم الأداء	عملية تقييم مدى تلبية مُخرجات نظام إدارة استمرارية الأعمال لمتطلبات وتوقعات الجهة.
الاختبار	نشاط أو إجراء يهدف لقياس قدرات وفعالية استراتيجية أو خطة معينة حسب معايير محددة سلفًا (ويجب أن يشمل عنصر النجاح أو الفشل).
الأصول الرقمية والتقنية	أي شيء مادي أو غير مادي له علاقة بتقنية المعلومات والبيانات الرقمية، مثل: الأجهزة والبرامج والتطبيقات والمنصات، والطابعات، ومكونات الشبكة التقنية، والأجهزة المحمولة، ورخص البرمجيات، والبيانات والمعلومات.
الخدمة الرقمية	مجموعة من الإجراءات الرقمية المرتبط بعضها ببعض لأداء وظيفة كاملة تُقدم من الجهة الحكومية للمستفيد من خلال القنوات الرقمية مثل البوابات الإلكترونية وتطبيقات الأجهزة الذكية، وتكون ذات مخرج رئيسي واحد معرّف ومحدد، ويمكن أن ترتبط مجموعة من الخدمات بعضها ببعض لتكوين منتج رقمي، مثل: إصدار الجواز وتجديد الجواز وتجديد رخصة قيادة والاستعلام عن المخالفات المرورية وتجديد الهوية الوطنية.
البرمجة الآمنة	لغات البرمجة والأكواد التي تحمي البرامج والبيانات من الهجمات السيبرانية والأخطاء والعيوب والفجوات التقنية.
الكود المصدري	مجموعة من الأوامر والتعليمات التي يتم كتابتها بلغة برمجة معينة لتحديد سلوك البرنامج أو التطبيق أو الخدمات الرقمية، وهو أساس تشغيل وعمل جميع المواقع الإلكترونية والبرامج والتطبيقات.
الإدارات ذات الصلة	جميع الأطراف (قطاعات وإدارات عامة وإدارات) داخل الجهة التي لها علاقة تشغيلية، أو لها اتخاذ قرار يتعلق بحوكمة تقنية المعلومات، مثل: إدارة المخاطر، وإدارة المشاريع، وإدارة الأمن السيبراني...الخ.
البرامج المساعدة الافتراضية	برامج تحاكي أجهزة التشغيل الفعلية، ويُسمح بتشغيل أنظمة تشغيل وتطبيقات مختلفة على نفس الخادم أو الجهاز.
الحاويات التقنية الافتراضية	تقنيات افتراضية تجعل تطبيقات الأعمال مستقلة عن موارد البنية التحتية لتقنية المعلومات لدى الجهة.
حزم البيانات	وحدات من البيانات التي يتم نقلها عبر شبكة الجهة، مما يسمح بتقسيم البيانات الكبيرة إلى أجزاء صغيرة، وإعادة تجميعها في الطرف المستقبل.
الهوية الشبكية	أصل أو مورد أو كيان فريد في الشبكة المعلوماتية، ويتم تمييزه عن طريق بروتوكولات الشبكة (TCP/IP) ليتم التواصل ونقل البيانات.

هيئة الحكومة الرقمية
Digital Government Authority

DGA.GOV.SA