قرار رقم 563 لسنة 2021 م اعتماد السياسة العامة للبريد الالكتروني للمؤسسات الليبية

نشر في نوفمبر 18, 2021

- التصنيف: القرارات
- تاريخ الإصدار: نوفمبر 18, 2021
- رقم الإصدار: 563
- جهة الإصدار: مجلس الوزراء
- القطاع: الاتصالات وتقنية المعلومات
- ذات الصلة: المعلومات والتوثيق
- الحالة: ساري

قرار رقم 563 لسنة 2021 م اعتماد السياسة العامة للبريد الالكتروني للمؤسسات الليبية

مجلس وزراء حكومة الوحدة الوطنية

- بعد الاطلاع على الإعلان الدستوري الصادر بتاريخ 3 أغسطس 2011 ميلادية، وتعديلاته.
- وعلى الاتفاق السياسي الليبي الموقع بتاريخ 17 ديسمبر 2015 ميلادي.
- وعلى مخرجات ملتقى الحوار الليبي المنعقد بتاريخ 9 نوفمبر 2020 ميلادي.
- وعلى قانون النظام المالي للدولة ولائحة مين الميزانية والحسابات والمخازن وتعديلاتهما.
- وعلى قانون رقم 4 1990 ميلادي، بشأن النظام الوطني للمعلومات والتوثيق.
- وعلى القانون رقم 12 لسنة 2010 ميلادي، بشأن إصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى القانون رقم 22 لسنة 2010 ميلادي، بشأن الاتصالات.
- وعلى ما قرره مجلس النواب في جلسته المنعقدة بتاريخ 10 مارس 2021 ميلادي، في مدينة سرت بشأن منح الثقة لحكومة الوحدة الوطنية.
- وعلى قرار اللجنة الشعبية العامة سابقا رقم 149 لسنة 1983 ميلادي، في إنشاء الهيئة الوطنية للمعلومات والتوثيق.

- وعلى كتاب السيد وزير الدولة للاتصالات والشؤون السياسية رقم 10676 المؤرخ في 30/8/2021
- وعلى ما قرره مجلس الوزراء في اجتماعه العادي السابع لسنة 2020 ميلادي.
- وعلى كتاب السيد أمين شؤون مجلس الوزراء رقم 16196 المؤرخ في 26/10/2021 ميلادي.

قرر

مادة 1

تعتمد السياسة العامة للبريد الالكتروني للمؤسسات الليبية المرفق بهذا القرار.

مادة 2

يعمل بهذا القرار من تاريخ دوري، وعلى الجهات المختصة تنفيذه.

مجلس الوزراء

18/11/2021

مادة (1)

المحتويات

- تمهيد
- الأدوار المحددة لتنفيذ السياسة العامة
- المتطلبات الأساسية لخدمات البريد الإلكتروني الرسمي
  - أولا/ الحماية:
  - ثانيا/ تأمين الوصول إلى خدمة البريد الإلكتروني:
  - ثالثا/ يلتزم مستخدمو خدمة البريد الإلكتروني في الجهات العامة أو الخاصة من الناحية الأمنية بما يلي:
- إدارة حساب البريد الإلكتروني
- مدير المكتب المخول
- نطاق البريد الإلكتروني والاستضافة الافتراضية
- استخدام كلمة مرور آمنة
- الخصوصية
- مسئولية الجهات العامة والمؤسسة الخاصة اتجاه المستخدمين
- نشر السياسة العامة للبريد الإلكتروني
- الاستخدام المناسب لخدمات البريد الإلكتروني
- الاستخدام الغير مناسب للبريد الإلكتروني

- قواعد المستخدمين
- إدارة مسائل الخدمة
- التدقيق في رسائل البريد الإلكتروني
- الحوادث الأمنية
- الملكية الفكرية
- تعطيل أو شطب أو إلغاء البريد الإلكتروني
- الإعفاء
- مراجعة حسابات خدمات البريد الإلكتروني
- مراجعة السياسة وتعديلاتها

تمهيد

تستخدم المؤسسة البريد الإلكتروني وسيلة رئيسية للاتصال تشمل بيانات المؤسسة التي تنقل بوصفها جزءا من المعاملات البريدية بين المستخدمين الموجودين داخل الدولة وخارجها، وتضع السياسة العامة للبريد الإلكتروني المبادئ التوجيهية والاسترشادية فيما يتعلق باستخدام خدمات البريد الإلكتروني الرسمية والجهة المعنية بالتنفيذ لخدمة البريد الإلكتروني الرسمية يتم تحديدها حسب الاختصاص والقدرة الفنية.

مادة (2)

تحدد السياسة العامة للبريد الإلكتروني قواعد وطرق وصول المستخدم إلى البريد الإلكتروني واستعماله وحمايته أثناء وبعد استخدام خدمات البريد الإلكتروني، ويكون المستخدم مسئولا عن استخدامه بطريقة تتسم بالكفاءة القانونية والفاعلية، كما تهدف السياسة العامة للبريد الإلكتروني إلى تفصيل المبادئ التوجيهية والاسترشادية للاستخدام الرسمي لنظام البريد الإلكتروني، وتساعد السياسة العامة للبريد الإلكتروني الجهات المستفيدة من خدمات البريد الإلكتروني في الحد من خطر الحوادث الأمنية المتعلقة بالبريد الإلكتروني والمراسلات الرسمية، ورفع الوعي العام بالاستخدام الأمثل للبريد الإلكتروني، وتعزيز الاتصالات الاقتصادية والتنموية والسياسية والإدارية بمختلف المؤسسات العامة بالدولة.

مادة (3)

تسري هذه السياسة بشكل استرشادي على جميع الموظفين والمستخدمين الذين يعملون ضمن فرق عمل أو إدارة من مهامها التواصل والمراسلة والتعاون المؤسسي، وذلك تنظيما لاستخدام البريد الإلكتروني أسوة بوسائط الاتصالات المختلفة.

تطبق هذه السياسة على موظفي الجهات العامة والمؤسسات والشركات العامة وموظفي البلديات، والبعثات الدبلوماسية الليبية، وأي جهة حكومية تستخدم خدمات البريد الإلكتروني في الدولة الليبية.

ويجوز للمؤسسات والشركات الخاصة والبعثات الدبلوماسية والمنظمات والمصارف العمل بهذه السياسة واعتمادها في العقود والاتفاقيات مع مستخدمو البريد الإلكتروني بالتوجيهات الواردة في هذه السياسة، كما يجوز للجهة العامة أو المؤسسة الخاصة اعتماد لائحة داخلية تسترشد فيها بهذه السياسة وفق ما تقتضيه إجراءات العمل وخصوصيته ودرجة تأمينه وسرعته، بما لا يتعارض مع السياسات المنظمة لاستخدام البريد الإلكتروني والسياسات العامة.

مادة (4)

يقصد بالعبارات والألفاظ الواردة في هذا القرار المعاني المبينة قرين منها، ما لم يدل السياق على خلاف ذلك:

1. المستخدم: يقصد به الموظف بالجهة العامة والمؤسسة والعاملين بالشركات الذين يملكون صلاحيات الوصول إلى خدمات البريد الإلكتروني الرسمية.
2. الجهة المعنية بالتنفيذ: هي الوزارة أو الهيئة أو المركز أو إدارة أو شركة عامة أو خاصة أو الهيئة العامة للاتصالات والمعلوماتية، أو مكتب أو إدارة تقنية المعلومات أو شركة تستوفي المعايير والشروط لتنفيذ الأعمال.
3. الجهات الحكومية: الوزارات والهيئات والمؤسسات وما في حكمها.
4. الإدارة المختصة: هي الإدارة التي يعمل فيها الموظفون أو الفريق المسئول عن اتخاذ وإقرار كافة القرارات المتعلقة بهذه السياسة في منظمتهم أو إدارتهم أو الجهة العامة أو الخاصة أو التجارية.
5. الموظف المسئول: هو المسئول عن جميع المسائل المتصلة بهذه السياسة، وهو الذي سيتولى التنسيق نيابة عن الجهة.
6. المؤسسة/ المؤسسات الخاصة: أي شركة خاصة أو قطاع أو نشاط تجاري تعود ملكيته لفرد أو مجموعة أفراد أو كيانات، ويخضع للقانون التجاري، ولديه نظامه الإداري والمالي الخاص به، أو منظمة غير حكومية أو غير ربحية NPO/NGO، أو مؤسسة مالية مثل المصارف والشركات المالية، أو منظمة أو سفارة أجنبية.
7. الشبكة الافتراضية الخاصة VPN: تمتد شبكة خاصة عبر شبكة عامة مثل الإنترنت، وهي تمكّن أجهزة الحاسوب من إرسال واستقبال البيانات عبر الشبكات المشتركة أو العامة كما لو كانت متصلة مباشرة بالشبكة الخاصة، مع الاستفادة من مزايا الاتصال المشفر والسرية والتحقق.
8. كلمة سر لمرة واحدة OTP: وهي كلمة سر صالحة لجلسة محددة أو وقت محدد، وتجنب المستخدم العديد من أوجه القصور المرتبطة بكلمات السر التقليدية (الثابتة) وغير المقيدة بزمن.
9. بروتوكول مكتب البريد POP: وهو بروتوكول يستخدم لاستجلاب البريد الإلكتروني من خادم البريد.
10. بروتوكول الوصول إلى رسائل الإنترنت IMAP: وهو بروتوكول يستخدم لاستعادة البريد الإلكتروني من خادم البريد عن بعد. على العكس من POP، فإنIMAP يعرض الرسائل على حاسوبك المحلي، ويخزنها على خادم البريد لدى خوادم أعدتها الجهة المعنية بالتنفيذ، حيث يسمح لك IMAP بمزامنة مجلداتك ومراسلاتك وبريدك مع خادم البريد الإلكتروني، وهذا غير ممكن باستخدام POP.
11. تعطيل الحساب Deactivation: يعني أنه لم يعد من الممكن الوصول إلى الحساب، وجميع رسائل البريد الإلكتروني المرسلة إلى حساب معطل يجب أن ترتد إلى المرسل، ويحفظ كل ما يوجد في هذا البريد لدى

الجهة المعنية بالتنفيذ.

12. التصيد الاحتيالي Phishing: هو محاولة احتيالية عادة ما تجرى عن طريق البريد الإلكتروني لسرقة المعلومات الشخصية المستخدم. رسائل التصيد الاحتيالي عادة ما تطلب من المستخدم النقر على رابط يأخذ المستخدم إلى موقع مشبوه أو خارجي أو ينفذ عملية في الخلفية، وتُطلب المعلومات الشخصية عن طريق الاحتيال والخداع. ولن تطلب الجهات القانونية والرسمية والشرعية هذه المعلومات عن طريق البريد الإلكتروني إطلاقا. يجب ألا ينقر المستخدمون على أي رابط، ويجب على المستخدم كتابة الرابط URL في المتصفح حتى إذا بدا الرابط حقيقيا.
13. الشبكة الداخلية Intranet: هي شبكة خاصة ذات تواصل محلي تكون داخل المؤسسة لسلامة الاستخدام الفعال لهذه السياسة، ولا يسمح للحواسيب المتصلة بالشبكة الداخلية بالاتصال بالإنترنت.
14. شهادة التوقيع الرقمي: هي ما يعرف بـ "شهادات الأمان والتشفير"، وهو مخطط رياضي لإثبات صحة رسالة رقمية أو مستند رقمي. تفيد هذه الشهادة بأن هذا التوقيع الرقمي الصحيح يعطي المتلقي سبباً للاعتقاد بأن البريد الإلكتروني قد أنشئ من قِبَل مرسل معروف، بحيث لا يستطيع المرسل أن ينكر أنه أرسل البريد الإلكتروني (التوثيق وعدم التنصل) وتضمن أن البريد الإلكتروني لم يتغير أثناء العبور (السلامة).
15. مفاتيح الأمان الفيزيائية: عبارة عن جهاز أو أداة إلكترونية صغيرة مثل الذاكرة القابلة للإزالة Flash Drive، يصادق على دخول الحسابات عبر إرسال رموز أمان مُبرمجة مسبقا والتعرف عليها، وتعمل مفاتيح الأمان على مستوى العتاد مثل جهاز منفصل ذي شاشة فيها أكواد متغيرة غير متصلة بالإنترنت، أو أي جهاز آخر، أو قطعة طرفية تتصل عن طريق تقنيات NFC، أو البلوتوث، أو الأزرار، لإرسال رموز الأمان.
16. التحقق الثنائي: هو طبقة أخرى من إجراءات الأمان تلي كلمة المرور، قد تكون على سبيل المثال مفاتيح أمان فيزيائية أو برمجية تقدم رموز دخول متغيرة وفق دالة زمنية، أو رسالة نصية تصل إلى رقم هاتف، أو رمز يصل إلى بريد إلكتروني آخر، جميعها متغير وعشوائي ومقيد بزمن معين، أو وجود العاملين معا وهما: كلمة المرور والتحقق الثاني.
17. الهيئة الوطنية لأمن وسلامة المعلومات: هي الجهة العامة المسئولة عن التدقيق والمراجعة في حالة وجود أي مخاطر أمنية عامة على المستوى الوطني، والإبلاغ عن المخاطر الأمنية السيبرانية، وإرسال التحديثات بذلك وإعداد السياسات واللوائح فيما يخص أمن المعلومات.
18. الهيئة العامة للاتصالات والمعلوماتية: هي الجهة المكلفة بتنظيم تقنية المعلومات والاتصالات في ليبيا، ومنفذ القوانين الصادرة عن الجهات التشريعية، ومن مهامها إصدار اللوائح التنفيذية لقوانين الدولة الليبية فيما يتعلق بالاتصالات وفق القانون رقم (22) لسنة 2010م.
19. تحقيق جنائي رقمي: هو تطبيق تقنيات التحقيق الجنائي والتحليل والبحث والتدقيق، لجمع الأدلة الرقمية من الأجهزة والحواسيب والهواتف الذكية والخدمات الإلكترونية والمواقع والشبكات، وعرضها على اللجان والهيئات المختصة لتقيمها وتقرير الأحكام المترتبة عليها وفق اللوائح والتشريعات النافذة.

مادة (5)

يعتبر استخدام خدمة البريد الإلكتروني المقدمة للجهات العامة والمؤسسات الخاصة التي تعتمد هذه السياسة في نظام العمل الداخلي موافقة من المستخدم على الخضوع لهذه السياسة.

كما تُمنح الخدمات المقدمة في إطار البريد الإلكتروني مجانا من الجهات العامة لكافة المسئولين والموظفين بالجهات العامة.

مادة (6)

الأدوار المحددة لتنفيذ السياسة العامة

تتولى الجهة المستفيدة من خدمة البريد الإلكتروني المقدم من الجهة المعنية بالتنفيذ تحديد الأدوار التالية في كل جهة عامة أو مؤسسة خاصة تستخدم خدمة البريد الإلكتروني، ويكون المكلف بتحديد الأدوار مسئولا عن إدارة قاعدة المستخدمين التي تشكلت في إطار هذا المجال، ويعتبر المكلف الافتراضي لهذه المهمة هو الجهة المالكة أو المستفيدة ما لم يحدد قرار أو سياسة أو قانون خلاف ذلك.

- تحدد الجهة العامة أو المؤسسة الخاصة الإدارة المختصة.
- تتولى الجهة العامة أو المؤسسة الخاصة تعيين الموظف المسئول.
- تحديد الجهة المعنية بالتنفيذ لخدمات البريد الإلكتروني.
- المؤسسات الخاصة والشركات الخاصة والتجارية والمنظمات غير الحكومية والمنظمات غير الربحية على النحو الذي يتماشى مع المعايير العالمية، ولا يضر بأسس ومبادئ هذه السياسة.

مادة (7)

المتطلبات الأساسية لخدمات البريد الإلكتروني الرسمي

أولا/ الحماية:

1. يجب ألا تكون هناك أي خدمة بريد إلكتروني أخرى موازية أو بديلة تعترف بها الجهات العامة أو المؤسسات الخاصة، أو تقرها أو تسمح بها هذه السياسة باستثناء الجهة المعنية بالتنفيذ، وتعتبر أي وسيلة تواصل موازية أو بديلة مخالفة لجميع قواعد ومبادئ هذه السياسة.
2. تلتزم الجهات العامة بنقل خدمات البريد الإلكتروني إلى الأنظمة المقدمة من الجهة المعنية بالتنفيذ في أسرع وقت ممكن، وفق معايير الجهة المعنية المنفذة وبما يتوافق مع هذه السياسة والسياسات واللوائح الداخلية، وذلك للاستمرارية ولتنفيذ موحد للسياسات في مختلف الجهات، ويُحتفَظ بعنوان البريد الإلكتروني السابق لمستخدمي الجهات العامة والمؤسسات الخاصة، حتى يتم نقل خدماتها وتنتشر على صعيد مؤسسي، وتُحدَّدُ مدة زمنية لعملية النقل، وفي حالة توفرت الإمكانيات التقنية، يجب نقل البيانات والمراسلات وجهات الاتصال والبريد الصادر والوارد والمسودات إلى الأنظمة التي أنشأتها الجهة المعنية بالتنفيذ، يستثنى من ذلك الجهات التي يصدر فيها قرار من الجهات القضائية أو الأمنية، أو المعفاة بموجب هذه السياسة.

ثانيا/ تأمين الوصول إلى خدمة البريد الإلكتروني:

1. على المستخدمين الذين يعملون في المكاتب والإدارات ذات المراسلات والبيانات الحساسة استخدام شبكة افتراضية خاصة "VPN" لتشفير الاتصال في قنوات خاصة، على ألا تكون الشبكة الافتراضية الخاصة مجانية أو عامة، وأن تكون مصممة خصيصا للأعمال ذات الطبيعة الخاصة أو السرية، مع وجود سياسة داخلية واضحة لاستخدام الشبكات الافتراضية الخاصة بالتشاور مع الجهة المعنية بالتنفيذ في حالة استخدامها.
2. تستخدم أنظمة التحقق الثنائي "2FA" بالجهات العامة أو المؤسسات الخاصة عن طريق تطبيق مستقل يستعمل أرقام الهاتف المحمول الموثقة لدى شركات الاتصالات المحلية بالدولة، من خلال الرسائل القصيرة، أو مفاتيح الأمان الفيزيائية Security Keys، بالإضافة إلى كلمة المرور، لضمان الوصول والسرية وهوية المستخدم.
3. يستخدم مسئول الحكومة أنظمة آمنة في التعامل مع الأجهزة المتصلة ببريده الإلكتروني في حالة وجوده خارج الدولة، والتعامل مع المعلومات الحساسة باستخدام التحقق الثنائي 2FA ، والشبكة الافتراضية الخاصة VPN للوصول إلى خدمات البريد الإلكتروني الحكومية، وفقا لما تراه الإدارة المختصة بأمن المعلومات والجهة المعنية المنفذة مناسبا في هذه الحالة.
4. تتبع السفارات بالخارج والبعثات الدبلوماسية الليبية اللوائح والسياسات المقررة من وزارة الخارجية في كيفية استخدام البريد الإلكتروني والتشريعات المعمول بها، وفقا لمقتضيات الحالة من جانب الإدارة المختصة.

ثالثا/ يلتزم مستخدمو خدمة البريد الإلكتروني في الجهات العامة أو الخاصة من الناحية الأمنية بما يلي:

1. اتباع السياسات ذات الصلة التي تضعها الهيئة الوطنية لأمن وسلامة المعلومات، والهيئة العامة للاتصالات والمعلوماتية، والمؤسسات التي تقر المعايير والمقاييس الخاصة بأمن المعلومات والمتعلقة بتصنيف المعلومات ومعالجتها وأمنها.
2. يجب استخدام شهادة التوقيع الرقمي لإرسال رسائل البريد الإلكتروني التي تعتبر مصنفة وحساسة، وتحديث أرقام الهواتف المحمولة المقترنة حاليا بالبريد الإلكتروني الرسمي للمسئولين لأسباب أمنية إذا استدعى الأمر وجود تحقق ثنائي عن طريق الهواتف المحمولة، ولا يستخدم الرقم إلا للإنذارات والمعلومات المتعلقة بالأمن التي ترسلها الجهة المعنية بالتنفيذ أو إدارة أمن المعلومات، بالإضافة لتحديث عنوان البريد الإلكتروني الشخصي ويفضل أن يكون من مزود خدمات داخل الدولة، إضافة إلى رقم الهاتف المحمول "من مزود خدمات اتصالات محلي"، ويحظر استخدام الأرقام المؤقتة المحلية أو الدولية.
3. لا يجوز للمستخدم تحميل أو تحويل أو رفع أو نسخ أو مزامنة رسائل البريد الإلكتروني من حسابه الرسمي للبريد الإلكتروني المعد مسبقا عن طريق برتوكول الوصول إلى رسائل الإنترنت IMAP أو POP على أي مزود آخر لخدمات البريد الإلكتروني، ولا يجوز له تقديم بيانات أو مراسلات أو معلومات أو جهات اتصال أو عنوان

البريد وكلمة المرور أو أي تفاصيل أخرى لحسابه على موردي خدمات البريد الإلكتروني الأخرى، سواء كانت تجارية أو شخصية أو عالمية أو عامة.

4. لا يجوز إعادة توجيه أي بريد إلكتروني مرسل إلى مستخدم عُطّل أو حُذِف حسابه إلى عنوان بريد إلكتروني آخر يمكن أن تحتوي هذه الرسائل محتويات تخص جهة عامة أو مؤسسة خاصة.
5. يلتزم الموظف المسئول توفير أحدث نظم التشغيل وبرامج مكافحة الفيروسات، وأن تكون التطبيقات محدثة على جميع الأجهزة، وأن تضاف كافة التحديثات والإصلاحات والإصدارات إلى نظام التشغيل كما توصي الشركة المقدمة لنظام التشغيل، بالتنسيق مع المستخدم، وفق ما توفره المؤسسة ويتناسب مع السياسات.
6. في حال اكتشاف حالة تسريب أو اكتشاف لعنوان البريد الإلكتروني دون رغبة في أن يكون هذا البريد متاحا للنشر من قبل أي وسيلة إعلامية، أو وسائل التواصل الاجتماعي، أو وكالات الأنباء، أو الإذاعات، أو الصحف، على أن يتم إرسال إنذار بواسطة البريد الإلكتروني إلى الشخص المعني.
7. في حال اكتشاف محاولة للحصول على كلمة المرور لحساب ما، يتم تنبيه المستخدم بواسطة الرسائل القصيرة على رقم الهاتف المحمول المسجل في سجلات الإدارة المسئولة عن إنشاء وحذف وتكوين وإعداد البريد الإلكتروني، وإذا لم يتخذ المستخدم الإجراء المطلوب بعد عدة تنبيهات تحددها الجهة المعنية بالتنفيذ مما يشير إلى وجود شبهة عملية قرصنة، يكون للجهة المعنية بالتنفيذ الحق في إعادة ضبط كلمة المرور الخاصة بالبريد الإلكتروني للمستخدم، مع تنبيه المسئول عن كل إدارة، على أن يتم فتح تحقيق جنائي رقمي بالأمر.

في حال حدوث قرصنة لهوية مستخدم من خلال عنوان البريد الإلكتروني أو كلمات المرور على قاعدة كبيرة من المستخدمين، أو على أمن البيانات أو الأمن السيبراني للمؤسسة، تقوم الجهة المعنية بالتنفيذ بإعادة ضبط كلمة المرور الخاصة بذلك المستخدم، ويُتخذ هذا الإجراء بشكل عاجل دون الرجوع إلى المستخدم، وتقدم المعلومات إلى المستخدم أو الموظف المسئول في وقت لاحق، وتكون الرسائل القصيرة SMS إحدى الوسائل للاتصال بالمستخدم، مع حظر أي وسيلة تواصل أخرى، ويجب على جميع المستخدمين تحديث أرقامهم الخلوية المسجلة في قاعدة إذا جرى التأكد من قرصنتها أو المساس بها أو إعلانها.

8. يتعهد مسؤول البريد الإلكتروني بالمؤسسة بعدم الاطلاع أو القيام بأي أعمال من نسخ أو نقل أو الاطلاع على البريد الوارد أو الصادر لأي مستخدم.
9. يُمنع إعادة توجيه بريد إلكتروني من عنوان البريد الإلكتروني الذي تقدمه الجهة العامة والمؤسسات الخاصة إلى بريد موظف شخصي خارج خدمة البريد الإلكترونية الحكومية لأسباب أمنية.
10. يتم استخدام عنوان البريد الإلكتروني الرسمي الذي توفره الجهة المعنية بالتنفيذ للاتصال بين المستخدمين فقط، سواء كان خاصا أو عاما داخل الجهة العامة والمؤسسة الخاصة أو خارجها، ويجب على المستخدم أن يدرك الحد الأدنى من المسئولية بشأن المحتويات التي ترسل كجزء من بريد إلكتروني.
11. لا يجوز الحفظ الآلي لكلمة السر في خدمة البريد الإلكتروني الحكومية لأسباب أمنية، ما لم تتوفر إجراءات سلامة معينة.
12. يمنع استخدام البريد الإلكتروني الرسمي في أي أغراض شخصية أو دعائية أو تجارية، أو التسجيل في خدمات بريدية لا علاقة لها بعمل الجهة العامة أو المؤسسة الخاصة، كما يُحظر تداول عنوان البريد الإلكتروني

على منصات التواصل الاجتماعي والمواقع الإلكترونية والمراسلات الخاصة، سواء كان عنوان البريد الإلكتروني الاسمي خاصا بالمستخدم نفسه أو أي مستخدم آخر.

مادة (8)

إدارة حساب البريد الإلكتروني

1. تقوم الجهة المعنية بالتنفيذ بإنشاء هويتين لعنوان البريد الإلكتروني بناء على طلب الجهة العامة أو المؤسسة الخاصة المعتمدة، إحداهما تستند إلى الاسم الشائع للجمهور والأخرى إلى الاسم الشخصي أو الهوية الحقيقية للمستخدم، على أن يتم استعمال الهوية التي تستند إلى الاسم الشائع من قبل الموظف الذي يتعامل مع الجمهور، واستخدام الأبجدية الرقمية والحرفية كجزء من هوية البريد الإلكتروني للمستخدم ذو الوظائف الحساسة، وفقا لما تحدده الإدارة المختصة، واتباع السياسة الداخلية لأسماء عناوين البريد الإلكتروني بالجهة العامة أو المؤسسة الخاصة على النحو المقدم إلى الجهة المعنية بالتنفيذ، أو بناء على اقتراحاتها.
2. يُسمح للموظف الحكومي الذي يستقيل أو يتقاعد الاحتفاظ بعنوان البريد الإلكتروني المستند إلى الاسم بعد الاستقالة أو التقاعد لمدة سنة واحدة، وفي وقت لاحق يوفر عنوان بريد إلكتروني جديد يحمل نفس هوية المستخدم مع عنوان نطاق مختلف من الجهة المعنية بالتنفيذ طيلة حياته، ويجوز له إعداد الرد الآلي لتوجيه المراسلين إلى البريد الشخصي المستحدث، ولا يجوز له اتخاذ القرار أو التصريح أو الموافقة على تعاقد.
3. يتم أرشفة بيانات عناوين البريد الإلكتروني المحذوف أو المشطوب أو المُلغَى ويُوقف عن العمل، ولا يتم الاطلاع على محتويات هذه البيانات إلا من طرف لجان مختصة بالتحقيق الجنائي الرقمي، المنصوص عليها في المادة (20) من هذه السياسة.
4. لا يجوز طباعة محتويات البريد الإلكتروني ولا يفصح عنها أو عن تواريخها أو موادها أو مرفقاتها خارج الجهة العامة أو المؤسسة الخاصة إلا بطلب قضائي أو رقابي، وتعتبر مخالفة ذلك إخلالا بسرية وخصوصية العمل.

مادة (9)

مدير المكتب المخول

يجوز للجهات العامة والمؤسسات الخاصة أن تستفيد من خدمة "مدير نظام" مخول من الجهة المعنية بالتنفيذ تكون له صلاحيات الإنشاء أو الحذف أو تغيير كلمة المرور الخاصة بالمستخدم، في إطار هذه الصلاحيات فقط وعند الضرورة، دون توجيه الطلب عبر نظام المراسلات أو الدعم الخاص بالجهة المعنية بالتنفيذ وفق لوائح داخلية، وعلى الجهات العامة والمؤسسات الخاصة التي لا تختار الحصول على المساعدة أن تحيل طلباتها بتفاصيل كاملة إلى وحدة الدعم بالجهة المعنية بالتنفيذ، حسب البريد الإلكتروني الذي تم الاتفاق عليه.

مادة (10)

تمنح الهيئة العامة للاتصالات والمعلوماتية الإذن للجهات العامة للحصول على أسماء نطاق: gov.ly، وللجامعات والمؤسسات والكليات التعليمية العالية والأكاديمية: edu.ly، مع السماح لها باختيار نوع وشكل الاستضافة، وعنوان النطاق الأنسب للبريد الإلكتروني.

ويجوز للجهات التابعة للجهات العامة، أو فروع الشركات، أو البعثات الدبلوماسية حجز اسم نطاق تابع لاسم النطاق الرئيسي للجهة العامة أو المؤسسة الرئيسية، مع إمكانية إنشاء موقع إلكتروني وأنظمة بريد إلكتروني منفصلة مع ذات الجهة المعنية بالتنفيذ.

مادة (11)

استخدام كلمة مرور آمنة

1. يجب على المستخدم عند إنشاء بريد إلكتروني جديد للمستخدم تغيير كلمة المرور الافتراضية في تسجيل الدخول الأول ويلتزم المستخدم لإعداد البريد الإلكتروني تغيير كلمة المرور الافتراضية الخاصة به.
2. على المستخدم الذي يحصل على خدمات البريد الإلكتروني استخدام كلمات مرور قوية تحتوي على حروف كبيرة وصغيرة وأرقاما ورموزا لتأمين حساب بريده الإلكتروني.
3. يجب تغيير كلمة المرور بشكل دوري وفق سياسة تسمى "سياسة كلمات المرور" تحددها الجهة العامة أو المؤسسة الخاصة داخليا.
4. يجب التحكم في سعة البريد الإلكتروني من خلال تحديد سعة الحصة المخصصة، ويعتبر كل مستخدم مسئولا عن تجاوز السعة المحدودة.
5. يلتزم المستخدم بأرشفة الرسائل المهمة بشكل دوري وحذفها من البريد الوارد.
6. على المستخدم الانتباه عند إرفاق المستندات أو الملفات بالبريد الإلكتروني، فقد تكون هذه المرفقات تابعة للآخرين، وإعادة توجيهها إلى مستلم آخر دون الحصول على إذن من المرسل يعتبر انتهاكاً لحقوق الملكية الفكرية، ويتحمل تبعاته من قام بإعادة التوجيه.
7. على المستخدم الانتباه عند فتح رسائل البريد الإلكتروني والمرفقات الواردة من مصادر غير معروفة، وضمان أن يكون محتوى البريد الإلكتروني دقيقا وواقعيا وموضوعيا، مع تجنب الآراء الشخصية حول الأفراد أو المؤسسات الأخرى.
8. يجب أن يدرك المستخدم رسائل البريد الإلكتروني قد تخضع للتدقيق للتأكد من أنها تلبي متطلبات هذه السياسة، وينطبق هذا على محتوى الرسائل والمرفقات والعناوين ورسائل البريد الإلكتروني الشخصية.
9. تعتبر جميع الرسائل المرسلة عبر البريد الإلكتروني بالجهة العامة أو المؤسسة الخاصة ملكية خاصة لها، ويشمل هذا رسائل البريد الإلكتروني الشخصية أيضا، ويجب ألا يكون لدى المستخدم أي توقع للخصوصية في أي شيء يقوم بإنشائه أو تخزينه أو إرساله أو استلامه على نظام البريد الإلكتروني الخاص بالجهة.

الخصوصية

1. يكون المستخدم مسئولا عن الحفاظ على سرية رسائل البريد الإلكتروني، وتتخذ الجهة المعنية بالتنفيذ الاحتياطات الممكنة للحفاظ على الخصوصية.
2. يجب على المستخدم ضمان عدم مشاركة المعلومات المتعلقة بكلمة المرور الخاصة بهم أو أي معلومات شخصية أخرى مع أي شخص أو جهة.
3. يجب على المستخدم التحقق من صحة المراسلات الواردة إليه والملفات المرفقة والروابط، وتجنب الدخول إلى أي محتوى مشبوه أو غير معلوم المصدر أو الاطلاع عليه، والتواصل على الفور مع الجهة المعنية بالتنفيذ عند استلام أي محتوى مشبوه.
4. يتم تصنيف المستخدمين في الجهة العامة من قبل الجهة المعنية بالتنفيذ إلى مستخدم عادي ومستخدم ذي وظيفة تتعامل مع بيانات حساسة تمس الدولة أو المواطنين، وبالتالي فرض سياسات التشفير على الأجهزة وعناوين البريد الإلكتروني، وتقييدها بشكل أكبر مقارنة بالمستخدم العادي.

مادة (13)

مسئولية الجهات العامة والمؤسسة الخاصة اتجاه المستخدمين

سياسة الامتثال:

1. تطبق الجهات العامة والخاصة المستخدمة للبريد الإلكتروني ضوابط داخلية مناسبة لضمان امتثال مستخدميها لسياسة البريد الإلكتروني. وتقدم الجهة المعنية بالتنفيذ المطلوب في هذا الشأن.
2. تلتزم الجهات العامة والمؤسسات الخاصة عدم إنشاء حسابات البريد الإلكتروني الرسمية لجميع مستخدميها إلا على خادم البريد الإلكتروني المقدم من الجهة المعنية بالتنفيذ، أو بواسطة الحلول الحديثة مثل الحوسبة السحابية كنوع من تكامل الأنظمة.
3. يتولى الموظف المسئول في الجهات العامة والخاصة المستخدمة للبريد الإلكتروني تسوية جميع الحوادث المتصلة بالجوانب الأمنية "السيبرانية" لسياسة البريد الإلكتروني، وتقدم الجهة المعنية بالتنفيذ الدعم اللازم لهذه التسوية.
4. تتولى الإدارة المختصة في الجهات العامة والمؤسسات الخاصة تنظيم برامج التدريب والتوعية بشأن أمن البريد الإلكتروني على فترات منتظمة، وتقدم الجهة المعنية بالتنفيذ الدعم اللازم لذلك.
5. يجب أن تحتوي كافة المراسلات المرسلة من طرف المستخدمين على إخلاء مسئولية أسفل البريد الإلكتروني المرسل.

مادة (14)

1. يجب على الإدارة المختصة في الجهات العامة والخاصة نشر سياسة البريد الإلكتروني وتحديثاتها وإصداراتها.
2. يجب رفع وعي الموظفين والمسئولين في مختلف الجهات العامة والمؤسسات الخاصة بكيفية استخدام البريد الإلكتروني، وتجنب عمليات التصيد الاحتيالي، والتحقق والكتابة الرسمية للبريد الإلكتروني.
3. يجب أن تستخدم الإدارة المختصة الرسائل الإخبارية ولوحات الإعلانات والنشرات الإلكترونية لزيادة الوعي بالسياسة العامة للبريد الإلكتروني وكيفية استخدامه بفاعلية.

مادة (15)

الاستخدام المناسب لخدمات البريد الإلكتروني

مادة (16)

يكون استخدام الاسم الشائع للجمهور في الاتصالات الرسمية، وذلك عند المراسلة من جهة عامة إلى جهة عامة عبر مراسلة مؤسسة خاصة لمؤسسة خاصة، كما يجوز استخدام الهوية المستندة إلى الأسماء في الاتصالات الرسمية والشخصية info@example.gov.ly IT.Manager@example.gov.ly.

الاستخدام الغير مناسب للبريد الإلكتروني

يكون الاستخدام الغير مناسب للبريد الإلكتروني في الحالات الآتية:

1. إنشاء وتبادل رسائل إلكترونية يمكن تصنيفها على أنها مضايقة أو مهددة أو منافية للعادات والتقاليد والقيم.
2. تبادل المعلومات ذات الملكية الفكرية والمعلومات السرية أو الحساسة دون السماح والإذن بذلك.
3. الوصول غير المصرح به إلى خدمات البريد الإلكتروني ويشمل توزيع رسائل البريد الإلكتروني دون الكشف عن هويتها، أو استخدام أجهزة الموظفين الآخرين، أو استخدام هوية مزيفة.
4. إنشاء وتبادل الإعلانات والعطاءات أو الامتيازات أو الهبات أو أي نوع من أنواع الاستفادة الشخصية وغير المؤسسية وليست من صميم العمل، والرسائل المتسلسلة، وغيرها من الرسائل الإلكترونية غير الرسمية.
5. إنشاء وتبادل المعلومات المخالفة للتشريعات، بما في ذلك قوانين حقوق التأليف والنشر.
6. النقل المتعمد لبريد إلكتروني يحتوي على فيروس حاسوبي أو برمجيات خبيثة أو برمجيات غير مرخصة أو روابط مشبوهة.
7. تشويه هوية مرسل البريد الإلكتروني أو انتحال شخصية وهوية مستخدم آخر.
8. استخدام حسابات الآخرين أو محاولة استخدامها دون إذن منهم.

9. إرسال رسائل إلكترونية تحتوي على عنصرية تجاه اللغة أو الدين أو الطائفة أو الانتماء العرقي أو إرسال رسائل إلكترونية شخصية إلى قائمة عناوين مجهزة مسبقا، أو تبادل رسائل إلكترونية تحتوي على رسائل غير اعتيادية أو إرسال رسائل إلكترونية ذات طابع عدواني أو تحريضي.
10. استخدام قوائم العناوين لغرض إرسال رسائل إلكترونية ذات طابع شخصي.
11. استخدام البريد الإلكتروني الرسمي في مشتريات أو حسابات بنكية أو تجارة شخصية أو تداوله على الإنترنت.

تعتبر هذه الحالات استخداما غير مناسب لحسابات البريد الإلكتروني الرسمي وانتهاكا للسياسة العامة قد تؤدي إلى تعطيل البريد الإلكتروني أو التحقيق الجنائي الرقمي تبعا لطبيعة الانتهاك تصل إلى المساءلة القانونية.

مادة (17)

قواعد المستخدمين

يكون المستخدم مسئولا عن بيانات البريد الذي يتم إرساله باستخدام البريد الإلكتروني الرسمي، وتعتبر رسائل البريد الإلكتروني والبيانات المرسلة عبر خادم البريد هي مسئولية المستخدم الذي يملك الحساب، ويحظر على المستخدم مشاركة كلمة المرور.

تشمل مسئولية المستخدم ما يلي:

1. يكون المستخدم مسئول عن الأنشطة في الأنظمة المخصصة لعملائهم باستخدام عناوين البريد الإلكتروني المخصصة لهم.
2. يجب استخدام "الرد على الكل" واستخدام "قوائم التوزيع" بحذر للحد من خطر إرسال رسائل البريد الإلكتروني إلى الأشخاص الخطأ.
3. تعتبر الجهة المعنية بالتنفيذ غير مسئولة عن البيانات المفقودة بسبب إجراءات المستخدمين، وعلى المستخدم أخذ نسخ احتياطية من الملفات المهمة على فترات منتظمة في حالة احتياجه لهذه الملفات والمراسلات، وبما لا يخالف أي سياسة داخلية خاصة بعمليات الحفظ وسرية البيانات.
4. يجب على مستخدم البريد الإلكتروني الرسمي للجهة العامة أو المؤسسة الخاصة التوقيع بالاسم والصفة الوظيفية وطرق التواصل من هاتف أو بريد إلكتروني أو تطبيق تواصل صوتي.
5. لا يجوز انتحال أو حذف أو تغيير المسمى الوظيفي إلا في حالة التغيير الإداري.
6. يجب توعية المستخدم أن استخدام البريد الإلكتروني الرسمي في مراسلات خارجية هو تمثيل للمؤسسة أو الجهة العامة وتمثيل للصفة الوظيفية للموظف.

مادة (18)

1. تلتزم الجهة المعنية بالتنفيذ بتوفير الحد الأدنى من مواصفات استقرار خدمة البريد الإلكتروني المقدمة للجهات العامة والمؤسسات الخاصة، وذلك بفرض الصيانة والتطوير الدوريين، والمراجعة والتحقق من سلامة البيانات، وإجراء الاختبارات اللازمة، وقياس مستوى الخدمة.
2. تلتزم الجهة المعنية بالتنفيذ بإقرار سياسة داخلية واضحة ومحددة التفاصيل لعمليات النسخ الاحتياطي ومواعيدها وطرقها ومحتوياتها وصلاحيتها وإجراءاتها وطرق استرجاعها، تسمى "سياسة النسخ الاحتياطي".
3. على الجهة المعنية بالتنفيذ التحقق بشكل دوري بأن المستخدم الذي لديه صلاحيات الدخول هو من يستخدم البريد الإلكتروني، وأن البريد الإلكتروني يعمل بشكل سليم في الإرسال والاستقبال.

مادة (19)

التدقيق في رسائل البريد الإلكتروني

لا يجوز للجهة المعنية بالتنفيذ أن توافق على المراجعة أو التدقيق الخارجي لفحص رسائل البريد الإلكتروني أو الإفراج عن سجلات الدخول بناء على طلب مؤسسة أو منظمة أو جهة أو شركة أخرى، باستثناء الهيئات القضائية والضبطية ذلك بعد أخذ الإذن من الجهات المختصة.

ويحظر الإفصاح عن سجلات الدخول والرسائل الإلكترونية للهيئات القضائية والضبطية وغيرها إلا بعد أخذ الإذن من الجهات المختصة.

مادة (20)

الحوادث الأمنية

يعتبر أي حدث ضار يمكن أن يؤثر على توافر البيانات وسلامتها وسريتها وإدارتها والوصول إليها حادثا، وتتخذ بشأنه الإجراءات الاتية:

1. يجب على الجهة المعنية بالتنفيذ إبطال مفعول أي ميزة أو خدمة من خدمات البريد الإلكتروني أو إزالتها إذا اعتبرت بمثابة تهديد يمكن أن تؤدي إلى قرصنة نظام البريد الإلكتروني الرسمي.
2. يجب على المستخدم عند ملاحظة أي حادث أمني أن يبلّغ الجهة المعنية بالتنفيذ وإدارة أمن المعلومات وتقنية المعلومات إن وجدت بالجهة العامة والمؤسسات الخاصة.
3. تؤخذ البلاغات الأمنية الواردة من الهيئة الوطنية لأمن وسلامة المعلومات والهيئة العامة للاتصالات والمعلوماتية ببالغ الأهمية، وتستقبل البلاغات عن الثغرات والمخاطر الأمنية من الجمهور والشركات إن وجدت، وتُحال إلى الجهة المعنية بالتنفيذ للنظر فيها واتخاذ الإجراء اللازم.

الملكية الفكرية

تخضع المواد التي يمكن الوصول إليها عن طريق خدمة البريد الإلكتروني الرسمي للجهة المعنية بالتنفيذ إلى سياسة الخصوصية أو الدعاية أو اتفاقيات الاستخدام أو منع الاستخدام، أو غير ذلك من الحقوق الشخصية والتجارية وحقوق الملكية الفكرية، وذلك وفقا للتشريعات النافذة بالخصوص، ولا يجوز للمستخدم استعمال الخدمات المقدمة في خدمة البريد الإلكتروني الرسمي بأي شكل من شأنه أن ينتهك هذه الحقوق أو يتعدى عليها بأي طريقة.

مادة (22)

تعتبر الجهات العامة مسئولة عن ضمان الامتثال لأحكام هذه السياسة، وعلى الجهة المعنية بالتنفيذ تقديم المساعدة التقنية اللازمة للجهات العامة.

يعتبر البريد الإلكتروني جزءا من المراسلات الرسمية، وتكون مسئولية إثبات صحته على الجهة المعنية بالتنفيذ، بواسطة مراسلة رسمية من الجهة العامة أو الخاصة الصادر منها أو الوارد إليها، ويجوز للجهات القضائية والقانونية الاستعانة بالأجهزة والهيئات واللجان والخبراء المحلفين في الجرائم الافتراضية ومكافحة جريمة تقنية المعلومات لإثبات صحة البريد الإلكتروني، تلتزم الجهة المرسلة استخدام أدوات التشفير لضمان عدم إمكانية التزوير أو تغيير المحتوى.

مادة (23)

تعطيل أو شطب أو إلغاء البريد الإلكتروني

1. في حالة وجود تهديد لأمن خدمة البريد الإلكتروني للجهات العامة، يجوز للجهة تعليق الخدمة أو إبطال مفعولها على الفور حتى يتم معالجة هذا التهديد، وعلى المستخدم إبلاغ الإدارة المختصة في تلك الجهة.
2. في حالة وجود تهديد لأمن خدمة البريد الإلكتروني في المؤسسات الخاصة، يجب على الجهة المعنية بالتنفيذ معالجة هذا التهديد أو الاستعانة بشركات متخصصة في هذا المجال.
3. في حالة وفاة المستخدم يكون التعامل مع البريد الإلكتروني وفق السياسة الداخلية للمؤسسة أو أن يتم تعطل البريد الإلكتروني أو إيقافه ونقل محتوياته إلى الأرشفة.

مادة (24)

الإعفاء

1. يجوز للجهات العامة التي لديها حاليا خوادم بريد مستقلة خاصة بها، بما فيها تلك التي تتعامل مع الأمن القومي مواصلة العمل بنفس الطريقة، بشرط أن تتم إضافة خوادم البريد الإلكتروني الموجودة داخل ليبيا، وأن يتم استيفاء شروط الأمن والسلامة الرقمية، وعليها ضمان اتباع مبادئ سياسة البريد الإلكتروني لتحقيق الاستخدام الموحد للسياسات داخل الدولة.
2. لا يجوز للبعثات والوظائف الدبلوماسية في الخارج الاحتفاظ بخدمات بريد إلكتروني بديلة تستضيفها خارج الدولة.
3. تستثنى من هذه السياسة الجهات التي تستخدم خوادم البريد على الشبكة الداخلية المفصولة عن الإنترنت.

مادة (25)

مراجعة حسابات خدمات البريد الإلكتروني

1. تتم المراجعة الأمنية لخدمات البريد الإلكتروني للجهات العامة وفقا للتشريعات النافذة في هذا الشأن المعمول بها والتي توصي بها الجهات المعنية بالتنفيذ، أو بما تراه مناسبا.
2. وتتم المراجعة الأمنية لخدمات البريد الإلكتروني للمؤسسات الخاصة بشركة أو هيئة مشهود لها بالتدقيق الأمني السيبراني بعد موافقة المؤسسة الخاصة.

مادة (26)

مراجعة السياسة وتعديلاتها

تتم مراجعة التعديلات وما يستجد من تقنيات وحلول تقنية حديثة على هذه السياسة وفق التشريعات المعمول بها، بما يضمن سهولة وانسيابية وإنتاجية العمل، ويحمي من المخاطر السيبرانية، وتصدر نسخة سنوية من السياسة بناء على اقتراحات من الجهات العامة والمؤسسات الخاصة.