أمن المعلومات

إن التطور الهائل الذي تعيشه المؤسسات والهيئات الحكومية في كيفية التداول الوظيفي المكتبي أو حتى الشخصي في مجال الحفظ والأرشفة والتداول والتبادل الالكتروني أصبح يتطلب الاحتفاظ بأرشيف لكل مادة سواء مكتوبة أو محوسبة أو ما يرده عبر البريد الالكتروني، مما عرضها بكثرة إلى الاختراق والتسريب لمعلومات دقيقة لهذه الوثائق المأرشفة، وقد أصبح ملحاً الحفاظ على أمن هذه المعلومات بكل الطرق والسبل المتاحة ما يعني اعتماد نظم تضمن جدية التطبيق لها.

بحيث يعتبر أمن المعلومات هو السياج الآمن من اللوائح والإجراءات التي يجب العمل في إطارها في كل زمان ومكان لغاية حمايتها.

وقد أصبح من المهم الافتراض أنه كلما كان هناك حرص على تأمين المعلومات من جانب مالكها يقابل ذلك حرص أكبر من طرف آخر مشبوه يسعى لاختراق هذا السياج الآمن لأهداف خاصة كالانتقام أو الانتفاع أو التشهير أو غيره.

الهيئة المحلية على اختلاف دوائر العمل فيها تستخدم الأنظمة الحاسوبية والشبكات والعديد من الوسائل التكنولوجية في تسيير أعمالها مواكبة لكافة المؤسسات والجهات على المستوى المحلي أو الدولي، ورغم ذلك لم ولن يتم الاستغناء عن التداول الورقي أو الوثيقة الرسمية في إتمام العمل، وكلا الجانبين يحتويان على كافة أشكال المعلومات العادية والمألوفة وغير العادية، يتطلب العمل بها أداء يختلف من وضع لآخر حسب طبيعة وأهمية أو دقة وحساسية هذه المستندات.

ولعل غاية أمن المعلومات في الهيئة المحلية هو الحفاظ على المستندات والمعلومات، حيث تمثل أوراقها الرسمية ومعاملاتها مجموعة بيانات أو وثائق تتمتع بأهمية أو حساسية بدرجة ما، طالما أنها خاضعة لنظام مؤسسة وتقدم الخدمات، وفيها موظفين قد يتفاوتون بحس المسؤولية والأمانة والشفافية.

وفي خضم التطورات الحاصلة، ووقاية من أن تحدث من حين لآخر محاولات (مشبوهة) منظمة أو غير منظمة للعبث بهذه المعلومات بمختلف أنواعها، إلا أنها تبقى في النهاية معلومات لها قوانين واختراقها والعبث بها وتسربها هو اختراق للنظم والقوانين المعمول بها.

وبما أن البيانات والمعلومات الخاصة بالهيئة المحلية هي محل عمل وحدة أمن المعلومات من حيث أمنها وسريتها وسبل الحفاظ عليها وطرق حفظها والتداول بها وتمريرها، فإن أمن المعلومات لدى بلدية المغازي يهدف إلى تحقيق التكامل العلمي والعملي بين عناصر الامن المعلوماتي وذلك من خلال:

أولاً: أمن المعلومات الورقية والمحوسبة:

1. أمن المعلومات والوثائق بأنواعها ودرجاتها تتمتع بخصوصية تستدعي حفظها بأمان.
2. الاتصالات والمراسلات الالكترونية أو المباشرة (مكتوبة أو مطبوعة) وثائق رسمية.
3. مدى درجة حساسية وسرية المعلومات والوثائق وصلاحيات تداول المعلومات، تمريرها من إلى ، وتأمين ذلك إداريا وقانونيا.
4. الرقابة الإدارية والاليكترونية على حاسوب المؤسسة وآلات التصوير الفاكس، الماسح وغيرها.
5. إجراءات تطبيق أمن الوثائق، قانونية، مؤسسية، إدارية، تكنولوجية، آليات خاصة.
6. الحفظ، الماهية وتعتمد على ثقل وحجم المعلومات وكيفية ذلك.
7. الإتلاف كيف ومتى وماذا نتلف من الوثائق وكيفية الإتلاف.
8. البيئة الوظيفية للموظف وحالة الرضا الوظيفي عنده ومدى أمانته وانسجامه مع عمله.

ثانياً: أمن الحواسيب:

على اعتبار أن الحواسيب هي الأدوات الأكثر استخداماً ليس فقط في المؤسسات بل على الصعيد الفردي واستخدامها رسمياً يتطلب اتخاذ كافة التدابير المتاحة لمنع اختراقها الكترونياً أو يدوياً وهو الأمر الذي يكون بعدة خطوات تعتمدها بلدية المغازي وفقاً لما يلي:

1. إغلاق الأجهزة المستخدمة سواء أكانت فردية أو مرتبطة بشبكة وتأمينها بكلمة سر بحيث يتم تشغيل شاشات التوقف المزودة بكلمات مرور على الحواسيب الرسمية، الحواسيب المحمولة (laptop) والخوادم للحيلولة دون عمليات الدخول المشبوهة.
2. عدم استخدام حاسوب من قبل أحد غير مشغله الرسمي إلا بإذن رسمي.
3. عدم استخدام صلاحيات وتسهيلات الوصول للبيانات خارج الصلاحيات المنصوص عليها.
4. ضرورة إغلاق الأجهزة بالشكل المألوف عبر إيقاف التشغيل أو الإيقاف المؤقت المشفر.
5. تأمين الشبكة التي تشمل الأجهزة الموصولة بها (سلكيا أو لاسلكيا) عبر الوسائل الممكنة لذلك.
6. عزل الطاقة عن الأجهزة عبر الموصل.

7. تركيب البرامج المضادة للفيروسات بتجهيز الشبكة والحواسيب بجدار حماية فعال منعا لأي محاولات تخريب.
8. عدم تنزيل أي من البرامج (غير المرخصة قانونياً) على الجهاز الرسمي.
9. عدم استخدام الجهاز لأغراض التسلية مثل تنزيل الألعاب والبرامج الترفيهية أو في الأمور الشخصية.
10. عند استخدام الانترنت الا لأغراض العمل على أن يكون مجهز بوسائل الحماية.
11. استشارة الوحدة المعنية بنظم المعلومات فوراً لدى ملاحظة أية أمور غير طبيعية خلال استخدام الانترنت.
12. عدم تحميل أو نسخ النصوص أو الصور أو المقاطع المجهولة والمثيرة لاحتمالية احتوائها على فيروسات أو محاولات من متطفلين.
13. عدم استخدام الحاسوب (الوظيفي أو الشخصي) والانترنت لمحاولة الدخول والتسلل إلى أجهزة وشبكات أخرى، وعدم استخدام الانترنت لإرسال مواد تحتوي على تهديد واستفزاز أو تحرش للآخرين.
14. في حال استخدام بريد الكتروني ينبغي مراعاة عدم إبقاءه مفتوحا لفترة طويلة ومن دون استخدام، كما يجب ان يكون الجهاز مزود بمضاد فيروس فعال لصد أي محاولات تخريبية.
15. في حال ورود أية رسالة مشبوهة لأي موظف يتوجب تنظيفها بمضاد الفيروسات أو إبلاغ الوحدة المعنية بنظم المعلومات.
16. عدم إعادة إرسال الرسائل الواردة والتي قد تحتوي على ملفات مشبوهة، والاستعانة بالوحدة المعنية بأنظمة المعلومات.
17. عدم فتح أية رسائل واردة غير معروفة أو غير متوقعة، وكذلك عدم فتح أو تنزيل أية ملفات مرفقة يشتبه في مصدرها.
18. عدم الدخول في نشاطات أخرى مثلا المشاركة بالرسائل البريدية الدعائية أو الرسائل المزعجة spam، أو الاجتماعية (التعارف أو الدردشة) أو غيرها من خلال الحاسوب الوظيفي.
19. عدم إرسال البرامج الضارة بأجهزة الحاسوب أو المساعدة على نشرها.
20. عدم تمرير أو التعاطي بكلمات السر/ المرور الخاصة بالجهاز أو بالشبكة بين الموظفين إلا بالإذن الرسمي بمعنى صلاحية رسمية من المسؤول ومن الطبيعي ان لا يتجاوز ذلك شخصين للوحدة.

أما بخصوص الحاسوب الوظيفي المحمول laptop فإنه للحفاظ على أمن المعلومات فيه إجراءات منها:

1. الحصول على تخويل رسمي باصطحاب الحاسوب المحمول لأغراض وظيفية.
2. عدم فتحه إلا في مكان مخصص للعمل.

3. في حالة السفر، يجب عدم ترك اللاب توب بدون متابعته في الأماكن التي يترك فيها.
4. يتوجب على المستخدمين المتنقلين الانتباه لدى استخدام خدمات الانترنت في الأماكن العامة.
5. عند فقدان أي حاسوب محمول laptop يحتوي على معلومات حساسة، أو حصول أي انتهاك آخر للحماية يجب القيام فورا بإبلاغ وحدة أمن ونظم المعلومات.

ثالثا: <u>أمن الوثائق:</u> لهذه الوثائق إجراءات عدة للحفاظ على سلامتها تتمثل فيما يلي:

1. الوثائق على اختلافها هي من ملك بلدية المغازي أو الدائرة التي تحمل اسمها.
2. أمن الوثائق يرتبط ارتباطا وثيقا بأمن المنشأة.
3. وجوب التعامل بطرق تداول الوثائق بأنظمة ولوائح عمل تحدد مسيرها.
4. في حال خرق الأنظمة واللوائح الناظمة لتداول الوثائق يجب الوقوف على هذا الأمر إدارياً وقانونياً باعتباره عمل غير مشروع.
5. سرقة او إخفاء أو تسريب أي وثيقة هو جرم أخلاقي وقانوني يعاقب عليه القانون.
6. كل حالة تزوير في الوثيقة تتطلب علاجاً خاصاً بها حتى يتم كشف التزوير، فهناك التزوير بإضافة أو إزالة صفحة كاملة والتي ممكن كشفها بالتتابع لتسلسل الكلام، أو بإزالة كلمة أو كلمات تخالف المعنى.
7. التزوير قد يكون بتصوير نسخة عن ورقة مع إضافات معينة وتزوير توقيع ما عليها لحالة أخرى.
8. عند التزوير بالإزالة لهدف غير مشروع يمكن كشفه بالأشعة الفوق بنفسجية أو مواد أخرى مختلفة حسب أهمية وحالة الورقة وحسب الإمكانيات.
9. التصوير بالأجهزة المحمولة والذكية بات من المخاطر التي تهدد نظرية أمن الوثائق مما يعني التعامل بحذر معها وبمعنى أدق التدقيق في نظام الأمن في عدم إدخال هذه الأجهزة إلى أماكن ومقرات حساسة.

رابعاً: <u>وسائل حفظ الوثائق:</u>

1. مكان ووضعية حفظ الوثائق هو من بديهيات تأمينها: وذلك باختيار حاويات أو خزائن ملفات مناسبة بعيدة عن الرطوبة وعن متناول أي كان عدا الموظف الرسمي المعني بذلك
2. يكون الحفظ بأسلوب التغليف والملف والتصنيف بمسميات واضحة وترقيمها وتأريخها أو تسميتها برموز لحاجات الامن المعلوماتي إن كانت حساسة.
3. بطبيعة الحال ينبغي إحكام إغلاق المكان بقفل أو بمفتاح رقمي سري حسب مستوى المعلومات المخزنة.

4. من ضروريات الحفظ حوسبة هذه الملفات أو حوسبة عناوين ملخِصة لها.
5. تحديد صلاحية الوصول والعمل بهذه الملفات، ويتم بصلاحيات رسمية وبقرار رسمي يسلم للمسؤول عنها.

خامساً: أمن البلدية ومقرها:

تحديد جوهر أمن البلدية يبدأ بتحديد مدى دقة عملها، وكذلك تحديد المخاطر التي تهدد البلدية من بشرية وغير بشرية ومقصودة من تخريب خارجي أو داخلي أو محاولات للسرقة، وغير المقصودة من حرائق وكوارث طبيعية وغيرها، أمن البلدية تحديدًا يعتبر السياج التنظيمي والإداري الذي تنبني عليه سلامة المؤسسة وتأمين المعلومات فيها، وأمن المنشأة بشكله العام هو ترتيب نظام الحماية وتأمين المنشأة على أسس ولوائح منصوص ومتفق عليها وفق توجيهات الجهات المختصة المعنية بتأمين البلدية.

سلامة الاحتياطات الأمنية والخدماتية مثل الدفاع المدني والإطفاء والإسعاف ومواجهة الكوارث والعمليات المضادة الفردية أو المنظمة تعزز من أمن البلدية وتحقق حالة أمنية لكل من يتواجد فيها.

ومن الضرورة بمكان أخذ كافة التدابير اللازمة للحفاظ على أمن البلدية وسلامة مقرها وذلك من خلال:

1. خضوع استقبال المراجعين لنظام محدد في وتنظيم عملية مراجعتهم لمقر البلدية.
2. توفير الراحة للمواطن المراجع لأن انعدام راحة المراجع يفضي الى عدم صبره على الانتظار وبالتالي التحرك في كل مكان.
3. لدى الحديث مع المواطن تم تهيئة مكان مخصص ومناسب لوقوفه أو جلوسه، بحيث يمكن ذلك دون الالتفات أو التمعن في أي وثائق سواء ورقية أو محوسبة، لمنع اطلاعه على معلومات لا تخصه وذلك من خلال مراجعته لقلم الجمهور مع تحويله إلى الدائرة أو القسم المختص ان لزم الأمر.
4. في حال انشغال الموظف عن المراجع يجب أن يكون هناك مكان مخصص للوثائق بعيد عن متناول الأيدي والحاسوب يتم إيقافه بإيقاف مؤقت لا يفتح إلا بكلمة سر.
5. الأوراق المبعثرة هنا وهناك تدل على عدم إتباع النظام وعلى فوضوية غير مقصودة للموظف يمكن لمهندس أو متطفل العبث بها.
6. من الضروري وجود مراقبة الكترونية يشرف عليها موظف أمن ويرجع ذلك لإمكانيات المؤسسة.
7. انتماء وإخلاص ودقة عمل الموظف يحفزه ذاتياً على إتباع نظام شخصي لتأمين الملف قيد العمل.

8. تخصيص مكان منفصل ومناسب لزائر مفترض للموظف تتحقق فيه المصلحة العامة والخاصة.
9. أمن البلدية يعني أيضا تأمينا من أي حالات اختراق أو تعدي أو هجوم مشبوه للتخريب بما يعنيه من إجراءات وقائية.
10. تزويد المنشأة بكل وسائل السلامة العامة والصيانة لكل أنظمة الأمان والمداخل والمخارج الآمنة وغيرها.
11. أمن المنشأة يعني الحفاظ على سلامة بيئة العمل، وإسناد إدارة أمن المؤسسة ومرافقها للجانب المعني بذلك وإذا أخل بواجبه يفترض معالجة الأمر كلياً.
12. توفير بيئة عمل مريحة ومناسبة لتحقيق أفضل أداء للموظفين عموماً بمن فيهم موظفي شرطة البلدية لإيجاد وضع أمني أمثل:

إن جودة الخدمة تنعكس ايجابياً على أمن البلدية وأمن المعلومات المتداولة فيها كونها تتم بين الكادر البشري والمواطن.

جودة التدابير الإدارية والأمنية يضفي هيبة العمل الوظيفي على المؤسسة ويدفع المواطن إلى احترام المؤسسة والتصرف فيها بلياقة وهدوء يؤدي الى انتظام التعامل بين الجميع، وانعدام ذلك يؤدي إلى التالي:

أ. التسيب واللامبالاة المقصود أو غير المقصود من الموظف.

ب. بيئة العمل غير المريحة من حيث المكان أو الخدمات يلغي الشفافية والمسؤولية.

ت. تلكؤ الموظفين في انجاز أعمالهم يؤدي الى تراكم العمل ووجود تبعات سلبية لذلك على أمن المؤسسة.

ث. عشوائية ومزاجية المراجعين لما لها من تأثير على سير العمل وعلى أمن المنشأة والموظفين.

ج. ضغط العمل والذي يرجع أحيانا الى سوء توزيع مهمات العمل بالشكل المناسب وما ينتج عنه من بعثرة وثائق وفوضى.

سادساً: <u>عمليات الإتلاف:</u>

1. عملية الإتلاف إجراء وظيفي تماماً ويرتبط عرفاً بالأوراق التي تم استنفاذ حاجتها.
2. المتلف يقابله حفظ وأرشفة سواء في الحاسوب أو النسخ.

3. يجب خضوع الإتلاف لنظام محدد من إدارة البلدية بلجنة مختصة يصادق على عملها من قبل رئيس المجلس البلدي.
4. خضوع هذه العملية الى قانون ولوائح يندرج في سياق حفظ أمن وسلامة المعلومات التي تحتويها الأوراق أو الملفات وبالتالي عدم تسريبها أو الاستفادة منها سلبيا من طرف ما، بمعنى أن ضابط هذا العملية ما يلي:

أ. **كيفية الإتلاف: تختلف كيفية الإتلاف باختلاف الجهة التي تتلف أي باختلاف المستوى وهي على النحو التالي:**

- **على المستوى الفردي:**

1. يقوم الموظف بإتلاف الأوراق وفق نظام وصلاحية متفق عليه بعد الانتهاء من تفريغ المعلومات على الحاسوب.
2. استخدام الفرامة المعتمدة لذلك ان وجدت.
3. الإتلاف بالحرق وإن لم يكن ذلك مناسبا يتم تمزيق الأوراق يدوياً بشكل كامل أي تمزيق ورقA4 بشكل طولي وتمزيق هذا الجزء لعدة أجزاء طولياً وعرضياً وهكذا دواليك مع بقية الأجزاء.
4. يساعد غرس المتلفات من الورق الممزق يدويا في الماء على تمام الإتلاف.
5. في حال كانت الأوراق تحتوي على معلومات خطرة يتم حرقها في مكان آمن بإشراف رسمي.
6. عند إتلاف الورق بالتفريم يراعى بعثرته إن احتوى على معلومات هامة.
7. مراعاة الجانب الإداري والقانوني لعملية الإتلاف.
8. المواد الصلبة التي لا منفعة منها يتم إتلافها حسب طبيعتها بشكل كامل ويتم التحقق منه.
9. اختيار مكان مناسب ومؤمن للإتلاف.

- **على مستوى لجنة الإتلاف:**

1. مصادقة لجنة الإتلاف على إتلاف الأوراق والمستندات والمواد الأخرى أقراص، صور وغيرها، والتأكيد على انتهاء حاجتها أو وجود نسخ رسمية لها ان تطلب الأمر ذلك.
2. تجميع ما تقرر إتلافه في صناديق أو حاويات معدنية مؤمنة.
3. التأكد من سلامة نتائج عملية الإتلاف للمواد المتلفة من النواحي البيئية والأمنية والتلف الكلي.
4. كتابة اللجنة تقرير رسمي بذلك لمسؤول المؤسسة بتوقيع أعضاء اللجنة.

5. إتلاف المواد على الحاسوب له تقنياته الخاصة والتي ينبغي القيام بها بلجنة من وحدة نظم المعلومات.
6. عملية إتلاف ملفات لا حاجة لها على الحاسوب تكون تقليدية عبر سلة المهملات وإفراغها تماماً.
7. ينبغي إجراء تفقد تقني بشطب كلي للملفات المتلفة أو معطياتها (Data)على الحاسوب بتعاون لجنة مختصة.
8. عند إجراء تبديل أو بيع حواسيب المؤسسة ينبغي التأكد من مسح جميع محتويات الحاسوب Format بما في ذلك الويندوز وجميع البرامج والملفات والتأكد من وحدات التخزين والقرص الصلب للحاسوب وتسليمه عبر لجنة مختصة وإجراء محضر رسمي.

سابعاً: <u>السلوك الشخصي للموظف على مسماه الوظيفي (حدود التعامل مع الآخرين):</u>

السلوك الأمثل لموظف يمكنه مستواه الوظيفي من معرفة معلومات بغض النظر عن طبيعتها في سياق أمن المعلومات يحتاج منه الالتزام بطابع سلوكي يلزم نفسه به ذاتياً، ليكون جزء من طبيعته وليس بحكم التعليمات

لذلك يجب الالتزام بالبديهيات الآتية:

1. الابتعاد عن الثرثرة والتقول بدون لزوم عما يعرفه.
2. عدم التطوع بتزويد أي شخص حتى أقرب المقربين له عن أي تحرك أو أي قرار بشأن أمور الوظيفة على الهاتف.
3. يكفي الرد بأنه سيتم الرجوع إليك أي (للمتصل) وطلب رقم هاتفه لذلك.
4. الالتزام بالسرية المطلقة والحدود الرسمية للإفصاح عن المعلومات:

أ. عدم الإخبار بالمعلومات الرسمية التي حصل أو اطلع عليها أثناء قيامه بوظيفته سواء كان ذلك كتابياً أو شفوياً أو الكترونياً، وقد صدر بشأن سريتها تعليمات أو قرارات صارمة.
ب. الامتناع عن الإدلاء بأي تعليق أو تصريح يتعلق بمواضيع ما زالت قيد الدراسة أو المداولة لدى المؤسسة أو الوزارة التي يعمل بها أو بغيرها.
ت. إعلام المسؤول بأي محاولات من أي شخص للحصول على معلومة ولو بالهاتف.

ث. عند نقل أي معلومة فإن الإفصاح عنها يتطلب موافقة أو تعليمات رسمية وبالحجم المسموح به وأن يكون نقل المعلومات يتناسق مع طبيعة العمل ولا يتعارض معه.

5. نظرا لأن طبيعة البعض هي الحديث مع أيٍ كان ليُظهر أنه على اطلاع على كل شيء، ينبغي ألا ينشر أي خبر أو معلومة سواء في جلسة اجتماعية أو في مركبة أو في مقهى أو غيره.
6. ضرورة عدم إبقاء أي ورقة أو وثيقة تخص العمل بحيازة الموظف إلا إذا كان لذلك ضرورة قصوى كاجتماع أو ابتعاث لمؤسسة أخرى وإعلام المسؤول بذلك.
7. على الموظف إزالة أي ورقة ليست قيد العمل ووضعها في ملفها أو مغلفها ومن ثم وضعها في مكانها المخصص وعند استخراجها يتوجب الحرص على وضعها ضمن مغلف أو دوسيه سواء كانت ورقة منفردة أو مجموعة أوراق.