- ممثل عن وزارة الدفاع الوطني،

- ممثل عن وزارة الداخلية والتنمية المحلية،

- ممثل عن وزارة تكنولوجيات الاتصال والنقل

أمر عدد 1250 لسنة 2004 مؤرخ في 25 ماي 2004 يتعلق بضبط النظم المعلوماتية وشبكات الهياكل الخاضعة إلى تدقيق إجباري دوري للسلامة المعلوماتية والمعايير المتعلقة بطبيعة التدقيق ودوريته وإجراءات متابعة تطبيق التوصيات الواردة في تقرير التدقيق.

إن رئيس الجمهورية،

باقتراح من وزير تكنولوجيات الاتصال والنقل،

بعد الاطلاع على القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية وخاصة الفصل 5 منه،

وعلى الأمر عدد 1248 لسنة 2004 المؤرخ في 25 ماي 2004 المتعلق بالتنظيم الإداري والمالي وطرق سير الوكالة الوطنية للسلامة المعلوماتية،

وعلى الأمر عدد 1249 لسنة 2004 المؤرخ في 25 ماي 2004 المتعلق بضبط شروط وإجراءات المصادقة على خبراء التدقيق في مجال السلامة المعلوماتية،

وعلى رأي المحكمة الإدارية.

يصدر الأمر الآتي نصه :

الفصل الأول ـ يضبط هذا الأمر النظم المعلوماتية وشبكات الهياكل الخاضعة إلى تدقيق إجباري دوري للسلامة المعلوماتية والمعايير المتعلقة بطبيعة التدقيق ودوريته وإجراءات متابعة تطبيق التوصيات الواردة في تقرير التدقيق، طبقا للفصل 5 من القانون المشار إليه أعلاه عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004.

الفصل 2 ـ تخضع إلى التدقيق الاجباري الدوري، طبقا للفصل 5 من القانون المشار إليه أعلاه عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004، النظم المعلوماتية والشبكات الراجعة بالنظر إلى الهياكل العمومية والنظم المعلوماتية وشبكات هياكل القطاع الخاص التالية :

- المؤسسات التي تشغل الشبكات العمومية للاتصالات ومزودي خدمات الاتصال والأنترنات،

- المؤسسات ذات الشبكات الإعلامية المرتبطة فيما بينها عبر شبكات خارجية للاتصالات،

- المؤسسات التي تتولى المعالجة الآلية للمعطيات الشخصية لحرفائها في إطار توفير خدماتها عبر شبكات الاتصالات.

الفصل 3 ـ تتم عملية التدقيق من خلال إجراء تحليل ميداني يعتمد العناصر الأساسية التالية :

- التحري حول النواحي التنظيمية وهيكلية السلامة وكيفية التصرف في إجراءات السلامة ومدى توفر آليات تأمين النظام المعلوماتي وكيفية استعمالها،

- التحليل التقني لسلامة كافة مكوّنات النظام المعلوماتي، مع اختبار مناعتها ضد كل أنواع المخاطر،

- تحليل وتقييم المخاطر التي قد تنجر عن استغلال الثغرات التي تم اكتشافها إثر عملية التدقيق.

الفصل 4 ـ عند الانتهاء من إجراء عملية التدقيق المشار إليها بالفصل 3 من هذا الأمر، يسلم الخبير المكلف بالتدقيق للهيكل المعني تقريرا يحمل ختمه وإمضاءه.

ويتضمن هذا التقرير خاصة ما يلي :

. وصفا وتقييما شاملا لسلامة النظام المعلوماتي يشمل الإجراءات التي تم اعتمادها منذ آخر تدقيق والنقائص المسجلة في تطبيق التوصيات،

. تحليلا دقيقا للنقائص التنظيمية والتقنية المتعلقة بإجراءات وآليات السلامة المعتمدة، يشتمل على تقييم للمخاطر التي قد تنجر عن استغلال الثغرات المكتشفة،

. اقتراح الإجراءات والحلول التنظيمية والتقنية للسلامة الواجب اعتمادها لتجاوز النقائص المسجلة.

الفصل 5 ـ تتولى الهياكل المشار إليها بالفصل 5 من القانون المشار إليه أعلاه عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004، القيام بالتدقيق في سلامة نظامها المعلوماتي وشبكتها بصفة دورية مرة على الأقل كل اثني عشر (12) شهرا.

ويمكن للوكالة الوطنية للسلامة المعلوماتية التمديد في هذا الأجل لأسباب استثنائية وبطلب من الهيكل المعني ثلاثة (3) أشهر على الاقل قبل حلول آخر أجل للقيام بعملية التدقيق.

الفصل 6 ـ يوجه الهيكل المعني تقرير التدقيق وجميع محاضر جلسات العمل التي يتم عقدها مع خبير التدقيق إلى الوكالة الوطنية للسلامة المعلوماتية بواسطة رسالة مضمونة الوصول أو وثيقة إلكترونية موثوق بها مع الإعلام بالبلوغ أو بالإيداع لدى الوكالة مقابل وصل إيداع في ظرف مغلق وذلك في أجل لا يتجاوز عشرة (10) أيام من تاريخ استلام تقرير التدقيق.

الفصل 7 ـ يمكن للوكالة الوطنية للسلامة المعلوماتية بعد دراسة التقرير أن تطلب من الهيكل المعني مدها بمعلومات أو وثائق إضافية والقيام بمراقبة ميدانية.

ويمكن للوكالة القيام بهذه المراقبة بعد إعلام رئيس الهيكل المعني بذلك بواسطة رسالة مضمونة الوصول أو وثيقة إلكترونية موثوق بها مع الإعلام بالبلوغ.

الفصل 8 ـ يمكن للوكالة الوطنية للسلامة المعلوماتية رفض تقرير التدقيق في الحالات التالية :

. عدم إنجاز التحليل الميداني وفقا للإجراءات المنصوص عليها بالفصل 3 من هذا الأمر،

. عدم تضمن تقرير التدقيق العناصر المنصوص عليها بالفصل 4 من هذا الأمر، أو إذا تبين للوكالة أن تقرير التدقيق لم يتضمن المعلومات الهامة المتعلقة بالنقائص المسجلة.

في حالة رفض التقرير، يتعين على الهيكل المعني إعادة إجراء التدقيق وموافاة الوكالة بالتقرير في أجل لا يتجاوز شهرين من تاريخ إعلامه بذلك.

وعند انقضاء هذا الأجل دون نتيجة، يمكن للوكالة تعيين خبير يعهد إليه بالتدقيق المشار إليه أعلاه على نفقة الهيكل المخالف.

الفصل 9 ـ تمنح هياكل القطاع الخاص المنصوص عليها بالفصل 2 من هذا الأمر مهلة لمدة اثني عشر (12) شهرا من تاريخ نشر هذا الأمر لتطبيق أحكامه.

الفصل 10 ـ وزير تكنولوجيات الاتصال والنقل مكلف بتنفيذ أحكام هذا الأمر الذي ينشر بالرائد الرسمي للجمهورية التونسية.

تونس في 25 ماي 2004.

زين العابدين بن علي