بيروت، في ٢٠٠٠/٨/١٨

تعميم رقم ٢٢٢

موجه إلى المصارف والمؤسسات المالية
ومؤسسات الوساطة المالية

الموضوع : دليل التوجيهات العامة المختصة بالقواعد التنظيمية
لأمان تكنولوجيا المعلومات.

درءاً للمخاطر المتنامية لتكنولوجيا المعلومات على المصارف والمؤسسات المالية ومؤسسات الوساطة المالية كافةً،

وحرصاً على تطبيق المعايير العالمية في إدارة شؤون المعلوماتية التي ترفع من مستوى الأمان،

تضع اللجنة بتصرّف هذه المؤسسات دليل :

"التوجيهات العامة المختصة بالقواعد التنظيمية لأمان تكنولوجيا المعلومات العاملة
في المصارف والمؤسسات المالية ومؤسسات الوساطة المالية"

وذلك بهدف اعتماد وتطبيق ما ورد فيه ضمن المهل الزمنية المشار إليها في جدول "مراحل تطبيق قواعد الأمان" من هذا الدليل.

ستنظم لجنة الرقابة لقاءً مع المؤسسات المعنية قبل نهاية شهر أيلول ٢٠٠٠ وذلك لشرح القواعد المطروحة وتوضيح آلية تطبيقها. وستوجه اللجنة بهذا الصدد دعوة رسمية تحدد فيها موعد وتفاصيل هذا اللقاء.

رئيس لجنة الرقابة على المصارف

وليد علم الدين

لجنة الرقابة على المصارف
مصرف لبنان

التوجيهات العامة المختصة بالقواعد التنظيمية لأمان تكنولوجيا المعلومات العاملة في المصارف والمؤسسات المالية ومؤسسات الوساطة المالية

الرقابة المعلوماتية
تموز ٢٠٠٠

التوجيهات العامة المختصة بالقواعد التنظيمية لأمان تكنولوجيا المعلومات العاملة في المصارف والمؤسسات المالية ومؤسسات الوساطة المالية

الفهرس

١. أهداف التوجيهات
٢. عمومية المبادئ والمتطلبات الخاصة لكل مؤسسة
٣. الميادين الأساسية لإرساء القواعد التنظيمية
٣,١ **الوظائف والمهام الإدارية**
٣,١,١. تسمية مسؤول عن أمان تكنولوجيا المعلومات
٣,١,٢. تسمية هيئة مسؤولة عن سياسة أمان تكنولوجيا المعلومات
٣,١,٣. في صلاحيات دخول الموظفين على النظام المعلوماتي
٣,١,٤. إدارة أمان تكنولوجيا المعلومات
٣,١,٤,١. منهجية الأمان وإجراءاتها
٣,١,٤,٢. ترتيب وتصنيف المعلومات وموجودات تكنولوجيا المعلومات الحساسة
٣,١,٤,٣. تطبيق قواعد الأمان على الاتفاقيات المعقودة مع الجهات المتعاملة مع المؤسسة
٣,١,٤,٤. مراقبة الدخول على النظام
٣,١,٤,٥. قيد معلومات الأمان في سجل خاص
٣,١,٤,٦. إعادة التقييم الدوري لأمان تكنولوجيا المعلومات
٣,١,٤,٧. سلامة المعلومات وبروتوكولات حيازتها وقراءتها

الفهرس

٣,٢. **الأجهزة**
٣,٢,١. إدارة الأجهزة
٣,٢,٢. في الاتفاقيات مع المورّدين
٣,٢,٣. أمور أمان الأجهزة
٣,٢,٤. المراقبة ورصد الخروقات
٣,٢,٥. صيانة الأجهزة والدعم
٣,٣. **أنظمة الاتصالات**
٣,٣,١. المبادئ العامة
٣,٣,٢. الاتفاقيات مع المورّدين
٣,٣,٣. في عمليات الاتصالات ومراقبتها
٣,٤ **البرمجة**
٣,٤,١. إدارة البرمجة
٣,٤,١,١. فصل المهمات
٣,٤,١,٢. جردة البرامج وملفات المعلومات
٣,٤,١,٣. تقييم أمان البرامج
٣,٤,٢. تخطيط وتطوير وكتابة وصيانة البرامج واختبارات القبول
٣,٤,٣. برامج الأجهزة
٣,٤,٤ إدارة الملفات وقواعد المعلومات
٣,٤,٥. البرامج التطبيقية

الفهرس

٣,٥. البيئة المحيطة بالأجهزة
٣,٥,١. نظام أمان مراكز الأجهزة المعلوماتية
٣,٥,١,١. في الترتيبات الإدارية
٣,٥,١,٢. في الترتيبات التقنية
٣,٦ العمليات
٣,٦,١. في إدارة العمليات
٣,٦,٢ في الموافقة على استعمال النظام
٣,٦,٣. في أمور العمليات اليومية ومراقبتها
٣,٦,٤ ضبط تبادل المعلومات (Input-Output Controls)
٣,٦,٥. في التدقيق والرقابة على العمليات
٣,٧. **في إدارة خزانة الوسائط المنقولة للمعلومات** (Removable Media)
٣,٨. **منهجية شراء أو تطوير الأنظمة المعلوماتية**
٣,٩. **خطط الطوارئ ومعاودة العمل**
٤. **الفترة الزمنية لتطبيق قواعد أمان تكنولوجيا المعلومات**
٤,١ مراحل تطبيق قواعد الأمان

١. أهداف التوجيهات

إن إرساء القواعد الصحيحة للتنظيم الداخلي في المؤسسات المصرفية والمالية ومؤسسات الوساطة المالية هو من أهم العناصر التي تساعد على زيادة الإنتاجية وضبط العمل داخليا" بشكل لافت وتؤسس لعلاقات متينة مع الجهات الخارجية المتعاملة معها ، كما تعزز مبادئ الأمان وبالتالي سلامة العمل.

ومع تشعّب الخدمات التي تقدمها الأسواق المالية والمصرفية ، وما تتطلبه من تقنيات واختصاصات مركّزة ، فإن القواعد التنظيمية لعمل المؤسسات تتطور معها ، مستفيدة" ومستعينة" بما تعرضه أسواق لوجستية الخدمات من أدوات ووسائل متخصصة لشتى متطلبات العمل. وبفضل هذه الأدوات ، أصبحت المؤسسات أكثر ديناميكية" لجهة رصد ومتابعة حيثيات العمل والاطلاع المستمر والدقيق على الأداء العام لوظائفها.

أن الوسائل المعلوماتية أضحت العصب الأساسي لأنظمة هذه المؤسسات ، فهي تضبط أعمالها وتساعد على استمرار نموّها. لكنها في الوقت نفسه ، تشكل هدفا" لإرباكات خطيرة إذا ما تعرضت لأي خلل أو ضعف أو خرق.

إن لجنة الرقابة على المصارف ، تهدف من خلال هذا المستند ، وكخطوة أساسية لتعزيز أمان العمل ، دعوة المؤسسات المصرفية والمالية ومؤسسات الوساطة المالية إلى إيلاء شؤون تكنولوجيا المعلومات كل عناية ، لما لهذا الموضوع من أهمية قصوى في الحفاظ على سلامة الأداء الوظيفي على كل الصعد. كما أن اعتماد المقاييس العالمية في التنظيم المعلوماتي الداخلي ، يوفّر المناخ التقني الصحيح للمؤسسات ويعزز المواصفات المطلوبة لدخول هذه المؤسسات الأسواق العالمية.

يتوجه هذا المستند ، بالدرجة الأولى إلى الإدارة العامة في كل مصرف ومؤسسة مالية ومؤسسة وساطة مالية ، لتتبناه ضمن سياستها التنظيمية ، وكذلك إلى المسؤولين المكلّفين إدارة شؤون المعلوماتية فيها وإلى اللجنة الإدارية للرقابة الداخلية ووحدة التدقيق الداخلي، للسهر على حسن تطبيقه وضمان احترام بنوده في كل نظام جديد أو معدّل.

٢. عمومية المبادئ والمتطلبات الخاصة لكل مؤسسة

ترتكز القواعد التنظيمية الأساسية المطلوب اعتمادها في هذا المستند ، على المقاييس العالمية لأمان تكنولوجيا المعلومات.

ففي حين أن هذه القواعد هي عامة ، فإنها لا تنفي خصوصية أوضاع ومتطلبات بعض المصارف والمؤسسات المالية ومؤسسات الوساطة المالية التي يمكن، ولضرورات عملية، أن تلجأ إلى تطوير هذه القواعد ، شرط ألا يخرق مبدأ الأمان والأهداف الأساسية لها.

تجدر الإشارة إلى أن بعض المهام الناتجة عن تطبيق هذه القواعد ، ربما تستدعي استحداث مراكز جديدة ، لكن هذا يتعلّق بحجم المؤسسة وتفرّعاتها العملية. إذ من الممكن في المؤسسات الصغيرة ، إسناد بعض هذه المهام إلى مسؤولين معيّنين دون اللجوء إلى استحداث مراكز أو وظائف إضافية. ومهما اختلفت أساليب العمل ، و كثرت المهام أو قلّت ، يجب أن تظل أهداف القواعد التنظيمية ثابتة ولا تتأثر بالحلول المعتمدة.

وفي حال توفّر عدة حلول لمسألة ما، على المصارف والمؤسسات المالية ومؤسسات الوساطة المالية اختيار الحل المناسب لأوضاعها التقنية والتنافسية.

إن هذا العمل التنظيمي يتطلب جهودا" كبيرة ومتواصلة ، ويمكن أن يؤدي إلى تعديل في الهيكلية التنظيمية للمؤسسة أو إعادة هندسة العمليات ، لكن هذه الجهود ستوفّر للمؤسسة لاحقا"، البنية الصحيحة لعمل سليم ، ونموّ مريح.

إن لجنة الرقابة على المصارف لن توفّر جهدا" لمعاونة القطاع المصرفي والمالي على إرساء هذه القواعد ، وبلورة المنهجيات الناجعة وتزويد هذه المؤسسات ، عند الحاجة، بمراجع المعلومات العلمية والتقنية.

٣. الميادين الأساسية لإرساء القواعد التنظيمية

إن الميادين التي تناولها هذا البحث ، حُدّدت حسب المفهوم التقني والمفهوم المهامي لشؤون المعلوماتية. فجاء التبويب على النحو التالي:
الوظائف والمهام الإدارية ، الأجهزة، أنظمة الاتصالات ، البرمجة ، البيئة المحيطة بالأجهزة، العمليات ، حفظ مخازن المعلومات ، شراء وتطوير أنظمة تكنولوجيا المعلومات ، خطط الطوارئ ومعاودة العمل ، الفترة الزمنية للتطبيق.

٣,١. الوظائف والمهام الإدارية

٣,١,١. تسمية مسؤول عن أمان تكنولوجيا المعلومات
(IT SECURITY OFFICER)

إن مهمة الإطلاع المستمر على أمن أنظمة المعلومات ، تتطلب من كل مصرف ومؤسسة مالية ومؤسسة وساطة مالية ، تسمية أحد المسؤولين لديها، الملمين بشؤون المعلوماتية ، للاهتمام بهذا الموضوع ، على أن يتولى المهام الأساسية التالية:

- التنسيق مع مفوّضي المراقبة في موضوع سلامة تطبيق القواعد الأساسية للأمان المعلوماتي الواردة في هذا المستند.
- تخطيط وتنفيذ وصيانة ومراقبة خطط الأمان وتطبيق المقاييس المعتمدة للتأكد من توزيع الصلاحيات الواضحة على الجسم الوظيفي بالشكل المطلوب، وعدم خرقها من أية جهة.
- القيام بالمراقبة الدورية لمنهجيات وقواعد تكنولوجيا المعلومات وخطط الطوارئ، أقله مرّة" واحدة في السنة.
- تحضير التقارير التقييمية الدورية وإيداع نسخة عنها مدير عام المصرف وحفظ نسخة أخرى.

- معالجة حوادث خرق الأمان والتأكد من الترتيبات المتخذة لعدم تكرارها.
- المشاركة في اختبارات خطط الطوارئ وخطط معاودة العمل.
- إبلاغ الإدارة العليا ومفوّضي المراقبة عن الحوادث الطارئة والمشاكل الآنية والممكن حدوثها لأمان المعلومات.
- وضع برامج توعية للموظفين حول الأمان المعلوماتي.
- اقتراح الخطوات الواجب اتخاذها في حال التجاوز على الضوابط الموضوعة لحماية أمان المعلومات.
- وضع آلية للاطلاع الفوري على مواد تكنولوجيا المعلومات تتضمّن التنبيه الفوري إلى الحوادث الطارئة ، وإذا أمكن بواسطة برامج متخصصة بالرصد المتواصل لأداء الأنظمة (On-Line Monitoring Audit Program).

٣,١,٢. تسمية هيئة مسؤولة عن سياسة أمان تكنولوجيا المعلومات

تعيّن الإدارة العامة للمصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية، هيئة مسؤولة عن سياسة أمان تكنولوجيا المعلومات ومهامها هي التالية:

- رسم السياسة العامة لأمان تكنولوجيا المعلومات وأطرها الزمنية والتقنية.
- التأكد من سلامة ترجمة وتنفيذ التوصيات المتخذة أو التدابير التصحيحية من قبل المسؤول عن أمان المعلومات.
- وضع القواعد الأمينة لتدمير أو إتلاف المعلومات القديمة والتي أصبحت بدون جدوى عملي أو قانوني للمؤسسة ، والسهر على حسن تطبيق هذه القواعد.
- تقديم المشورة حول الخطوات الواجب اتخاذها في حال تجاوز إحدى ضوابط الأمان.
- الإطلاع على الاتفاقيات المعقودة الخاصة بتكنولوجيا المعلومات للتأكد من مراعاتها شروط الأمان الموضوعة من قبلها.
- وضع أطر عقود التأمين المختصة بمخاطر تكنولوجيا المعلومات.

٣,١,٣. في صلاحيات دخول الموظفين على النظام المعلوماتي

نظرا" لأهمية المعلومات المحفوظة في الأنظمة المعلوماتية المعتمدة في المؤسسات المصرفية والمالية، وتفاديا" لإمكانية التصرّف بها خارج الصلاحيات الممنوحة، يتوجب إرساء قواعد دخول الموظفين على هذه المعلومات ووضع الضوابط لها، على أن تراعى فيها النقاط التالية:

- وضع قواعد تحدّد الصلاحيات الممنوحة للموظفين للدخول والعمل على الأنظمة المعلوماتية وفقا" لطبيعة عمل ورتبة كل موظف.
- إعداد لوائح تفصّل أسماء الموظفين ، وطبيعة عملهم ، ورتبهم ، والصلاحيات المحددة لكل منهم وفقا" لطبيعة عمله على النظام المعلوماتي.
- إعداد كتيب عن نظام الأمان المتّبع يشرح قواعد الأمان الخاصة بالمؤسسة وكيفية الإبلاغ عن حالات خرق نظام الأمان في حال حدوثها ، واعتباره مرجعا" لكافة الموظفين، خاصة" الجدد منهم.
- إعداد دورات تدريبية لكل فئة من الموظفين ، بهدف عرض وشرح مبادئ الأمان المعلوماتي (الإداريين، المسؤولين عن العمليات، المسؤولين عن برمجة النظام، المدققين ، الخ...).
- اتّباع سياسة تبديل المهام بين الموظفين بشكل دوري.
- وضع منهج يشرح بالتفصيل الخطوات الواجب اتّباعها في حال تمّ أي تبديل في الوظائف (كتبديل في طبيعة العمل أو تعديل في المركز والصلاحيات أو إنهاء خدمات الخ...) وكيفية تعديل الصلاحيات الممنوحة للموظفين وفقا" للتبديل الذي حصل.

٣,١,٤. إدارة أمان تكنولوجيا المعلومات

٣,١,٤,١. منهجية الأمان وإجراءاتها

على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية:
- أن يطوّر ويضع منهجيات أمان مكتوبة.
- وأن يوثّق إجراءات تطبيقها في مكتبة مفهرسة.

٣,١,٤,٢. ترتيب وتصنيف المعلومات وموجودات تكنولوجيا المعلومات الحساسة

- قبل البدء بالعمل بأيّ نظام ، يجب إعداد مستند يبيّن تصنيف الأمان لمواده المختلفة ، من أجهزة وبرامج وعمليات وشبكات اتصالات وأمكنة ومواقع حفظ ، وللشروط التي تمكّن من استعمالها ، والتي تتيح إجراء التعديلات عليها.
- على كل مصرف ومؤسسة مالية ومؤسسة وساطة مالية أن تضع دليلا" لكيفية إدارة المعلومات والموجودات يبيّن بوضوح تلك الحساسة منها.
- يجب أن يحتوي الدليل على كل أنواع تطبيقات المعالجة في بيئة تكنولوجيا المعلومات ، وأن يتم مراجعته سنويا" ، وأن يكون بمتناول المسؤول عن أمان النظام.
- يجب أن تُقيّم هذه الموجودات بالنظر لعدة معايير ، وأهمّها:
  - سرّيتها (Confidentiality)
  - سلامتها (Integrity)
  - توفّرها للاستعمال (Availability).

٣,١,٤,٣. تطبيق قواعد الأمان على الاتفاقيات المعقودة مع الجهات المتعاملة مع المؤسسة

- على المصارف والمؤسسات المالية ومؤسسات الوساطة المالية أن تضمّن الاتفاقيات المبرمة مع الموردين ، بنودا" واضحة" حول كيفية التعامل والشروط التي تلزم هؤلاء على احترام تعهّداتهم.
- على هذه المؤسسات أن تحدّد بوضوح الخدمات والمعلومات والأجهزة التي يمكن أن تطالها هذه الاتفاقيات، وأن تخضعها لمتطلبات الأمان التي تعتمدها.
- على هذه المؤسسات أن تتأكد من أن الجهة الخارجية التي تتعامل معها تحترم بنود الأمان التي تشير إليها الاتفاقيات المعقودة ، خاصة" لجهة أساليب العمل لدى الجهة الخارجية ، ووعي مسؤولية الأمان التي يتحملها موظفوها في تنفيذ الخدمات ، كأعمال الصيانة المختلفة.

٣,١,٤,٤. مراقبة الدخول على النظام

- إن الدخول على النظام ومصادر المعلومات يجب أن يعالج بالنظر لمجموعات العاملين فيه:
  - المستعملين (Users)
  - القيّمين على العمليات (Operations Personnel)
  - القيّمين على صيانة النظام والدعم (Maintenance and Support Personnel)
  - المحللين والمبرمجين (System Analysts and Programming Personnel).

- على كل من يعطى صلاحيات للدخول على النظام ، أن يوقّع على بيان، يعلن فيه عن فهمه للقرارات والقوانين التي أصدرتها المؤسسة بهذا الخصوص، ويتعهّد باحترامها وتنفيذها. يبقى هذا التعهد ساري المفعول بعد ترك الموظف المعني عمله ، وللفترة الزمنية التي تجيزها القوانين.

- على القوانين والقواعد التي ترعى الدخول على النظام ومواد تكنولوجيا المعلومات ، أن تنظّم المهام المختلفة وتحدد صلاحيات الهيئات المسؤولة عنها ، وبالأخص:
  - الجهة المخوّلة إصدار وتعديل التعليمات والأوامر المرتبطة بتشغيل النظام (Command Procedure and Configuration Control)
  - الجهة المسؤولة عن إدارة كلمات السرّ وأدوات الدخول على النظام مثل أجهزة الترميز والمفاتيح وبطاقات الدخول (Encryption Keying Material, Keys, Locks, Access Cards)
  - الجهة المخوّلة تعديل أو إضافة أو إلغاء معلومات من بيئة العمل الفعلية (Production Environment)
  - الجهة المخوّلة الدخول أو الإطلاع على معلومات البرامج (Access to Software Sources)
  - الجهة المخوّلة تعديل أو إضافة أو إلغاء أي أداة أو معلومة من أجهزة أو برامج الاتصالات
  - الجهة المسؤولة عن وضع التقارير بما يخصّ حوادث الأمان
  - الجهة المكلفة تحديد صلاحيات كل فرد فيما يختص بأوقات الدخول على النظام، وتحديد أماكن التواجد المسموح بها ، وكذلك الملفات والبرامج المسموح الدخول إليها
  - الجهة المكلّفة السهر على احترام حقوق نشر المواد المعلوماتية والملكية الأدبية
  - الجهة المخولة إعطاء الإذن بنقل الأجهزة والبرامج بصورة مؤقتة أو نهائية من مكان إلى آخر
  - الجهة المسؤولة عن حماية الأجهزة والبرامج من الخروقات المختلفة ومن البرامج الخبيثة (Virus)

- الجهة المسؤولة عن آلية التأكد من استعمال الأجهزة والأنظمة بما يتوافق مع القوانين والقواعد المرعية.

٣,١,٤,٥. قيد معلومات الأمان في سجل خاص

إن التدابير الواجب اتخاذها لقيد هذه المعلومات تتلخص بما يلي:

- وضع لائحة بالمستعملين المصرّح لهم بالدخول على الأنظمة ومصادر المعلومات ، كل حسب نطاق عمله.
- يجب أن يوضّح هذا القيد:
  - أنواع الأنشطة والعمليات والحدث المسبب لها (Events Nature)
  - طريقة متابعة هذه الأنشطة
  - تاريخ الإبلاغ عن محتوى هذه القيود.
- وضع آلية لقيد حوادث الأمان التي تطال بيئة تكنولوجيا المعلومات وكيفية الإبلاغ عنها للجهة المختصة.
- وضع مستند لقواعد الأمان الواجب اتباعها من قبل الموظفين لتمكينهم من مراجعتها والتقيّد بها ، وبالتالي إدراكهم لماهية حوادث الأمان.
- تسجيل كافة حوادث الأمان بالتفصيل في سجل خاص وكذلك الخطوات التي نفّذت لمعالجتها، وطريقة إطلاع الإدارة العامة عليها.

٣,١,٤,٦. إعادة التقييم الدوري لأمان تكنولوجيا المعلومات

- على كل مصرف ومؤسسة مالية ومؤسسة وساطة مالية أن تستعين بفريق عمل متخصص بأمور أمان المعلومات، لإجراء تقييم شامل لقواعد الأمان المتخذة ، مرّة كل ثلاث سنوات على الأقل بصورة روتينية، وبصورة فورية بعد أي حادث مهمّ أو خرق لأمان النظام.

- كما يجب إعادة التقييم جزئيا" أو كليا" حسب الحالة المستجدة، مثلا":
  - تعديل جغرافي في مواقع الأجهزة
  - تعديل في هيكلية النظام (Reconfiguration)
  - تعديل في معطيات شبكة الاتصالات
  - تعديل في تصنيف الحساسية لبعض المعلومات أو الأجهزة
  - تعديل في طبيعة أو أداء العمليات.
- يجب أن تبلغ نتائج التقييم الموضوع من قبل الفريق المختص، والذي يتضمن الخطوات الواجب اتخاذها لمعالجة الأمر، إلى الإدارة العليا التي تحوّلها بدورها إلى الجهاز المكلّف بالمعالجة، والذي يفيد الإدارة دوريا" عن التقدّم الحاصل.

٣,١,٤,٧. سلامة المعلومات وبروتوكولات حيازتها وقراءتها

إن مبدأ فصل المسؤوليات يشكّل إحدى ركائز الأمان الأساسية، بحيث لا يعطى فردا" واحدا" حق الإدارة الكاملة لإحدى عمليات تكنولوجيا المعلومات الحساسة.

وعلى هذا الأساس يجب أن يطبق مبدأ الفصل هذا، على الأمور التالية:

- **البرمجة**
- **الأجهزة**
- **النظم التشغيلية**
- **الشبكات**
- **العمليات ومحيط العمل الفعلي**
- **التجارب**
- **الصيانة.**

كذلك على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تعمل على ألا يقوم فرد واحد بكل مراحل إحدى العمليات الحساسة (Sensitive Operation) ، فمثلا" يجب فصل مهمة إدخال المعلومات عن مهمة معالجتها داخل أجهزة الحاسوب.

وحفاظا" على مبدأ الأمان هذا ، على المسؤولين حاملي مفاتيح ومهام معلوماتية حساسة (Sensitive Data)، أن يعوا أهمية الحفاظ على سريتها ، والتأكد من عدم استعمالها ، من قبل أي كان أثناء دخولهم على النظام (بواسطة مفاتيحهم).

٣,٢. الأجهزة

٣,٢,١. إدارة الأجهزة

إن جردة الأجهزة ومتابعتها باستمرار ، تتطلب التدابير التالية:

- وضع لائحة بكل الأجهزة والمعدات (Units) التي تضاف إليها والوصلات بينها والأجهزة الطرفية والقنوات مع تفاصيل مواصفاتها مثل:
  - المورّد (Vendor)
  - النوع (Model Number)
  - الرقم المتسلسل (Serial Number)
  - معلومات عن آخر إصدار (Revision Level)
  - معلومات عن برمجتها الداخلية (Micro-Code Level)
- الإشارة إلى تركيبة الأجهزة الدنيا التي تمكّن من تلبية الخدمات الحساسة الضرورية للمؤسسة في الحالات الطارئة.
- مسك ملف لمتابعة شؤون الصيانة ، مبوّب بالأجهزة وتواريخ الصيانة.

٣,٢,٢. في الاتفاقيات مع المورّدين

يجب أن تتضمّن الاتفاقيات مع المورّدين العناصر الأساسية التالية:

- مستند تركيبة الأجهزة وكل التعديلات التي تطرأ عليها.
- المعلومات الوافية لتعليمات استعمال الأجهزة.
- بروتوكولات الصيانة العادية وكذلك التلبية السريعة للمشاكل الطارئة.
- الترتيبات الضرورية لحماية المعلومات ، والمحافظة على أمان النظام ، أثناء عمل موظفي الصيانة.

٣,٢,٣ أمور أمان الأجهزة

أهم الأمور الواجب تطبيقها بهذا الخصوص من قبل كافة المصارف والمؤسسات المالية ومؤسسات الوساطة المالية:

- اعتماد أمكنة آمنة لكافة الأجهزة والتمديدات، بطريقة تحميها من الحوادث الممكنة أثناء أعمال الصيانة أو التنظيفات.
- إذا ما توفّرت إمكانية إقفال الأجهزة ، يجب المحافظة على ذلك طوال وقت تشغيلها.
- في حال عدم استعمال الأجهزة لوقت طويل نسبيا"، خلال دوام العمل أو في حال تعرّضها لظروف غير ملاءمة ، كرطوبة عالية أو طاقة كهربائية غير مستقرة، من المستحسن أن يكون لهذه الأجهزة إمكانية التوقّف الذاتي.
- عندما تكون لوحات وأزرار التحكّم بالأجهزة معرضة لحوادث عدم الانتباه، يجب حمايتها من الاستعمال السهل ، وإبعادها "قدر المستطاع" عن المتناول القريب.
- عندما يكون التحكم بالأجهزة عن بعد (Authorized Remote Users) ، على الأنظمة أن تتمكّن من تحديد المستعمل بشكل فردي ، عن طريق التعرّف على الجهاز المتصل إذا أمكن ، إما بواسطة:
  - البطاقة الذكية (Smart Card)
  - أجهزة اتصالات مغلقة وضمن أماكن آمنة (Dedicated Communications in Secured Location)
  - شيفرة محصّنة (Approved Encryption Methods)

• يجب أن تفحص تدابير حماية الأجهزة دوريا" ، للتأكد من عدم إمكانية تنفيذ بعض العمليات لغير المصرّح لهم بها ، ومنها على سبيل المثال لا الحصر:

- الدخول على النظام ومصادر المعلومات (System and Data Resources)
- الدخول إلى مناطق حفظ النتائج والتقارير في أجهزة الحاسوب (Residual Data)
- الدخول إلى مناطق غير مسموح بها في الذاكرة ومخازن المعلومات

(Outside Allocated Memory Bounds).

٣,٢,٤. المراقبة ورصد الخروقات

• على النظام أن يتمتع بإمكانية إصدار تقارير عن استعمالات الأجهزة (Hardware Maintenance Logs) ، تحتوي أقله على المعلومات التالية:

- الإشارات الصادرة عن الأجهزة (Machine Checks)
- جدول بالعمليات والتعليمات المنفّذة
- محاولات نقل المعلومات
- الحالات الطارئة وغير العادية للبيئة المحيطة
- حوادث الطاقة وتقلّباتها
- أخطاء أخرى.

٣,٢,٥. صيانة الأجهزة والدعم (Hardware Maintenance and Support)

في أعمال الصيانة:

• يجب أن يعيّن كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية مسؤول يقوم بالإشراف على أعمال فريق صيانة المورّد ،أثناء قيامه بعمله ، على أن يكون ملمّا" بأمور المعلوماتية ، ليتمكّن من التأكد من صحة ودقّة الصيانة المنفّذة وعدم دخول فريق الصيانة على مناطق ومعلومات معيّنة محظّرة داخل الأجهزة.

- يجب اتخاذ التدابير اللازمة لعدم السماح بالدخول إلى مناطق المعلومات والملفات عند القيام بأعمال صيانة الأجهزة عن بعد (Remote Link-Up For Maintenance Purposes).
- يجب توثيق كل أعمال الصيانة في سجل خاص ، والاحتفاظ به لمدة سنتين على الأقل ، من تاريخ حصولها.

فيما يتعلق بالحوادث الطارئة على الأجهزة:

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تضع آلية مكتوبة للإبلاغ عن حوادث الأجهزة وطرق متابعة معالجتها.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تبلّغ إلى المسؤول عن أمان تكنولوجيا المعلومات عن حوادث الأجهزة التي تؤثر على قواعد الأمان، فور حدوثها.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تضع تدابير طوارئ، تحدد أولوية المعالجات والخطط البديلة المتّبعة وبالتالي أولوية صيانة الأجهزة الحساسة.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تؤمن مصادر بديلة للطاقة وتفرعاتها، تلجأ إليها عند توقف المصادر الأساسية عن العمل، كأجهزة ضبط الطاقة (UPS)، وجهاز الوصل الأرضي (System Grounding)، والتأكد دوريا" من حسن أداءها.
- إن كل تعديل في الأجهزة، يجب أن يحوز على الإذن المسبق وأن يوثّق وأن يحفظ في سجل خاص.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن أي عملية تعديل أو إضافة أو إلغاء في الأجهزة ، لا ولن تؤثّر على قواعد الأمان المتبعة.

٣,٣. أنظمة الاتصالات

٣,٣,١. المبادئ العامة

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تقرر وتراقب بواسطة سلطة مركزية الصلاحيات الممنوحة لتمكين المستعملين من الدخول على الشبكة وتوثيق هذه الصلاحيات.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تعيد تقييم نظام أمان الاتصالات ، بصورة دورية وتتابع تطورات التكنولوجيا في هذا الموضوع، للتنبّه إلى طرق الخرق الممكنة والمستجدة.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تضع البرامج التي تلبي في تفصيلها متطلبات أمان الاتصالات ، من شروط السرية وسلامة المعلومات وحيازتها ، مثل اعتماد كلمات سرّ محصنة ووسائل ضبط الأخطاء وتصحيحها وأن توفّر وسائل نقل بديلة (Alternate Routing).

٣,٣,٢ الاتفاقيات مع المورّدين

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن الاتفاقيات المعقودة مع المورّدين تتضمن تفاصيل خريطة الشبكة
(Communication Configuration Chart).
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن التعديلات التي تجرى على نظم الاتصالات تحافظ على قواعد الأمان الموضوعة من قبل المؤسسة.

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن أي تعديل يطال أي جزء من نظام الاتصالات ينال موافقة الجهة المخوّلة قبل تنفيذه، وأن تراقب وتوثّق هذا التعديل في سجل خاص يوضع لدى المسؤول عن أمان تكنولوجيا المعلومات.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تضع جردة بأجهزة الاتصالات وبرامجها وخطوط تناقلها، على أن تحتوي على المعلومات التالية:

- **Communications Hardware and Services**
  - circuits, lines or connections and the identification of the supplier,
  - the location of the physical termination of the circuits and lines,
  - media used (e.g. coaxial, fiber, unshielded twisted pair),
  - the circuit or line status (assigned or available),
  - the level of security classification or designation of each circuit or line,
  - hardware identifiers of remote input/output units,
  - communications hardware (document model number and serial number modems, dial-ins, concentrators, packet switched devices),
  - encryption devices, and data switches.

- **Communications Software and Data**
  - software programs,
  - configuration database and files (libraries),
  - software procedures (Command Files),
  - software utilities,
  - security components,
  - license numbers.

- **Communications Networks**
  - devices, servers, routers, gateways, bridges,
  - protocol and level,
  - network operating systems and applications software,
  - network media and transmission methods,
  - identification of node names (document name, network address, type, location, responsible manager).

٣,٣,٣. في عمليات الاتصالات ومراقبتها

على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تدوّن وتوثّق القواعد التي تتحكم بعمليات الاتصالات، على أن تتضمن تفصيل العمليات كافة ومن أهمها:

- communications start-up,
- communications shut-down,
- equipment operation,
- enabling/disabling/switching specific communications links/lines/ports,
- backup procedures/requirements, configuration data and software,
- maintenance,
- handling of sensitive material,
- emergency situations,
- communications logs review,
- the use of network performance monitoring and reporting,
- the use of network management systems utilities.

إن عملية مراقبة عمليات الاتصالات ، يجب أن ترصد أخطاء وحوادث الاتصالات ومن أهمها:

- protocol errors,
- inconsistent communications identification data as related to hardware identification and polling responses,
- sequence errors,
- status and error alarms,
- data inconsistencies,
- communications access control errors,
- errors in network applications, (E-mail, Electronic Data Interchange (EDI), file transfer, proxy accounts, routing).

٣,٤.البرمجة

٣,٤,١.إدارة البرمجة

٣,٤,١,١.فصل المهمات

عملا" بمبدأ فصل المسؤوليات، على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تعهد المهام التالية، قدر الإمكان إلى أشخاص مختلفين:

- برمجة الأجهزة (System Programming).
- إدارة النظام (System Administration).
- برمجة التطبيقات (Application Programming).
- اختبارات القبول (Quality Assurance and Acceptance Testing).
- صيانة مكتبات البرامج (Program Library Maintenance).

على أن توثّق هذه المهمات تفصيليا" في سجل يحفظ لديها.

٣,٤,١,٢.جردة البرامج وملفات المعلومات

على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تعمل باستمرار على صيانة جردة البرامج، لتعطي الصورة الفعلية لمقوّمات النظام، على أن تندرج تحت الأقسام التالية:

- برامج الأجهزة (System Software).
- برامج إدارة قواعد المعلومات (Database Software).
- البرامج التطبيقية (Application Software).
- البرامج المساعدة للنظام (Software Utilities).
- ملف أوامر استعمال النظام (Software Procedures and Command Files).

- ملف أوامر استعمال البرامج التطبيقية (Program and Procedure Libraries).
- قواعد وملفات المعلومات (Databases and Data Files).
- ضوابط هيكلية التطبيقات (Operational Configuration Parameters).

على أن يشار في هذه الجردة، إلى معلومات وافية عن كل برنامج أو ملف مثل:

- درجة حساسية البرنامج أو الملف.
- الشروط التي تحكم صيانته.
- المسؤول عن صيانته.
- عدد النسخ ومواقعها.
- الأشخاص المصرّح لهم استعماله.
- تاريخ وضعه في الخدمة وتواريخ التعديلات اللاحقة عليه.

٣,٤,١,٣. تقييم أمان البرامج

على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تقيّم دوريا" أمان البرامج لما لهذا التقييم الدوري من أهمية في الحفاظ على قواعد الأمان وسلامة العمل ، وهو يرتكز بصورة أساسية على:

- المناهج والممارسات العملية.
- التوافق مع المقاييس المتّبعة في المؤسسة.
- إدارة برامج النظام والبرامج التطبيقية.
- التأكد من مراعاة مبدأ فصل الصلاحيات وعدم استعمال برامج من قبل أشخاص غير مصرّح لهم بذلك.
- تدابير الطوارئ المختصة بالبرامج وملفات المعلومات.
- دقة جردة البرامج والملفات على أنواعها.

٣,٤,٢. تخطيط وتطوير وكتابة وصيانة البرامج واختبارات القبول

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتبع قواعد وبروتوكولات مدوّنة لكافة البرامج الجديدة لديها ، ليتمّ على ضوءها كتابة البرامج المستحدثة وقبولها واختبارها ووضعها في الخدمة وصيانتها وحمايتها.
- إن التدقيق في توافق البرامج الجديدة مع مقاييس الأمان المتّبعة ، يجب أن يتمّ مع تقدم كل مرحلة أساسية من مراحل النظام المستحدث.
- إن كل تعديل في برامج بيئة العمل الفعلي ، يجب أن يخضع لآلية محددة تؤدّي للنفاذ الصحيح ، ومنها:
  - طلب التعديل
  - الموافقة على طلب التعديل
  - قيد ومتابعة الطلبات غير المنجزة
  - تفصيل للحلول المعتمدة تتضمّن على الأخص ، المدة المطلوبة لإنجازها ، الإمكانيات المتوجبة لها ، طريقة الحل والتأثيرات على التطبيقات الأخرى وعلى خطط الطوارئ
  - نتائج الاختبارات بعد إجراء التعديل المطلوب
  - الموافقة على إدخاله بيئة العمل الفعلي
  - إدخاله بيئة العمل الفعلي.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية عدم الاختصار في شمولية التجارب، حتى ولو كانت البرامج محضّرة خارج المؤسسة ومعتمدة لدى مؤسسات أخرى.
- يجب صيانة برامج العمل الفعلي الأساسية (Source) منها ، والمنفّذة (Executable) في بيئتها المنفصلة عن بيئة البرمجة والتطوير.

- إن كل خطأ أو حادث يطال البرامج أو قواعد المعلومات ، يجب أن يبلّغ فورا" للمسؤول عن أمان النظام ، وأن يدوّن كذلك مع تفاصيل التاريخ والساعة وطبيعة الحادث.
- إن صيانة مكتبات البرامج (Software Library Maintenance) ونقلها ونسخها يجب أن تكون موثّقة ، لتكون مأمونة في حال إعادة استعمال نسخ معيّنة ، ولا تؤدي إلى الوقوع بأي التباس أو خطأ.
- إن آلية توزيع البرامج للاستعمال في أقسام المؤسسة أو للإفادة منها عن بعد، (Distributed or Remote Systems) يستوجب التقيّد بالقواعد الأساسية التالية:
  - قانونية التوزيع ووجهة الاستعمال المطابقة للاتفاقيات مع المورّد
  - المحافظة على نسخة موحّدة وصيانتها في كل أماكنها (Unique Version in Distributed Systems)
- يجب أن تخضع عملية قبول البرامج المستحدثة لآلية مكتوبة ، تحتوي في مضمونها على العناصر التالية:
  - قواعد ومقاييس اختبارات القبول
  - الاعتبارات المطلوبة لتأكيد جودة البرامج المستحدثة
  - الإفادة عن نتائج الاختبارات لتأكيد مطابقتها لمقاييس القبول المطلوبة.
- يجب الامتناع عن استعمال معلومات بيئة العمل الفعلية في عمليات التجارب، وفي حال تعذّر ذلك ، يجب اتخاذ التدابير اللازمة للمحافظة على السرية المطلوبة عند استعمالها.
- يجب أن يتمّ اختبار البرامج في بيئة منفصلة عن بيئة العمل الفعلية.
- عندما تحوّل البرامج المستحدثة أو المعدلة إلى بيئة قبول البرامج أو إلى بيئة العمل الفعلية، يجب إعادة تأليف وتجميع البرامج المنفذة، (Recompile and Reassemble the Executable Programs)
  وذلك بغية التأكد من مطابقة آخر نسخة عن البرامج الأساسية مع تلك المنفذة (Compatibility Between Source and Executable Programs).

- يجب التأكد، من ضمن التجارب وحيث ما ينطبق الحال ، من خلوّ البرامج من الجراثيم الطارئة أو المقصودة.

٣,٤,٣. برامج الأجهزة

- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن برامج الأجهزة تتمتّع **بقدرة التعرف** على مكونات ومحيط النظام ، ومنها:
  - المستعملين (Users)
  - المعلومات (Data)
  - الوسائط (Media)
  - البرامج (Programs)
  - وحدات الأجهزة (Hardware Components)
  - أجهزة الاتصالات (Communication Links).
- وأن تتمكن من قراءة تعريف الوسائط (Volume Labels) ومقارنتها مع المعلومات التي ترد في طلبات الدخول إليها (Access Requests).
- على برامج الأجهزة أن تحمي المعطيات السرّية بواسطة شيفرة أمينة (One-Way Encryption Method).
- في حالات البيئة المشتركة (Multi-User Environment)، يجب أن تؤمن برامج الأجهزة **عزل** مستعمل عن آخر ومستعمل عن جهاز آخر للحؤول دون حدوث المشاكل التالية:
  - التغيير في معطيات النظام وخصوصيته
  - تأثير مستعمل على ملفات أو بيئة مستعمل آخر
  - إيقاف النظام بطريقة مقصودة أو عن طريق الخطأ

ومن جهة أخرى ، على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تنظّم الدخول واستعمال البرامج والملفات المشتركة.

- على برامج الأجهزة ، أن تتيح المحو الكامل لمناطق من ذاكرة الأجهزة ومن الوسائط الداخلية والخارجية الممغنطة ، إثر الاستغناء عن المعلومات الحساسة في داخلها.
- على برامج الأجهزة ، أن تتمكّن من إيقاف الأجهزة الحساسة تلقائيا" في حالات عدم الاستعمال الطويل ، للحؤول دون استعمالها من قبل غير المصرّح لهم بذلك.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتأكد من أن قواعد **مراقبة الدخول على النظام تتيح** لبرامج الأجهزة أن:
  - تسجل أي دخول على الأجهزة أو المعلومات
  - تعلم المستعمل للجهاز عن تاريخ آخر استعمال له ، والمحاولات الفاشلة للدخول إليه ، إذا وجدت
  - تدير الإمكانيات الممنوحة للمستعملين ، من قراءة وكتابة وإلغاء للمعلومات، وكذلك البرامج التي تمكنهم من الدخول إليها
  - تتعرّف على مجموعات المستعملين المختلفة (Owner, Group, System, etc…)
  - عند رفض أي دخول غير مسموح به ، يجب ألا تعطى تفاصيل ومبررات هذا الرفض.
- في حال **الحساسية العالية** لبعض الأجهزة ، وكي لا تؤثر أية حوادث طارئة على استمرارية العمل ، على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتخذ **التدابير الاحترازية** الأساسية التالية:
  - اللجوء إلى تجهيز مجموعة ثانية من الأجهزة والبرامج وأجهزة الاتصالات، تكون مكرّرة للأجهزة الأساسية أو الأولية (Primary System) وبمثابة أجهزة رديفة (Alternate System)، تقوم بنفس وظائف الأجهزة الأولى وبنفس الوقت وتكون جاهزة للحلول مكانها في حال تعطّلها أو توقّفها عن العمل لسبب ما.

- على الأجهزة الرديفة ، أن تتابع العمليات بصورة آلية ، عند حدوث عطل أو توقف في الأجهزة الأولية.
- على برامج الأجهزة ، أن تتمكن من رصد وقيد كل حدث على الأجهزة والنظام ومنها:
  - Jobs status (entry, processing, completion, deletion, restart, and abort),
  - File, volume, and database accesses,
  - Communications device accesses,
  - Network messages,
  - User log-on and log-off,
  - System operator commands and responses,
  - System messages (start-up, shutdown, abort),
  - Requests regarding system configuration changes,
  - System logging facility status (start, stop, alter, print, dump, delete, rename and overflow),
  - Changes to access control information,
  - Changes to lists of authorized users,
  - Detected security incidents.
- على أن يتمّ توثيق المعلومات الوافية لكل حدث ، مثل:
  - طبيعة ونوع الحدث
  - التاريخ والساعة
  - تعريف المستعمل
  - تعريف الجهاز (Device Identification)
  - تعريف المهمة أو العملية.
- كما يجب أن يرسل النظام بمعلومة عن الحادث ، إلى لوحة التحكم الرئيسية (System Console) ، وأن يصدر في الحالات الشديدة الخطورة ، إشارات صوتية فورية ، للفت الانتباه في وقت مبكر.

٣,٤,٤ إدارة الملفات وقواعد المعلومات

لا بدّ من تأكيد أهمية إدارة ملفات وقواعد المعلومات (Data Files & Databases)، لما تتضمّنه من مقوّمات النظام، لذا على المسؤول عن هذه الملفات (Database Administrator) أن يلحظ آلية مراقبة سلامة المعلومات وحمايتها من البرامج الخبيثة ويضع شروط نسخها أو نقلها من مكان إلى آخر بهدف استعمالها أو بهدف صيانة الأقراص الصلبة الممغنطة أو الضوئية التي تحتويها، أو اقتطاع أجزاء منها بسبب عدم قدرة استيعابها لمعلومات إضافية.

- إن المسؤوليات التي تترتّب على إدارة الملفات وقواعد المعلومات من قبل هذا المسؤول ، تتلخص بالأمور التالية:
  - قواعد التحكم باستعمالها (Access Control)
  - فهرس المعطيات (Data Dictionary)
  - تعريفها وتواجدها (Definition and Creation)
  - سلامتها وعملية مراقبتها (Integrity and Audit)
  - نسخها وعملية ترميمها (Back-Up and Recovery).
- يجب العمل على مبدأ عزل المعلومات ، بطريقة تحفظ سريتها.
- يجب وضع آلية لتدقيق متانة المعلومات (Logical and Physical Consistency)، ورصد التناقض والأخطاء داخل قواعد وملفات المعلومات (Lost Records, Open Chains, and Incomplete Sets).
- يجب أن يساعد فهرس المعلومات على توحيد مقاييس أسماء واستعمالات هذه المعلومات.
- يجب أن يحظّر استعمال برامج صيانة المعلومات ، قدر المستطاع ، وإلا أن توضع في إطار المراقبة الدقيقة في حال اللجوء إليها.

- يجب أن يتمكن النظام من تصحيح قواعد المعلومات تلقائيا" ، بعد كل حادث توقف.
- يجب المحافظة على مبدأ تعدد تواجد المعلومات ، من خلال النظام الثانوي أو الرديف ، وذلك عن طريق وضعه كنسخة ثانية ، ضمن بيئة تخضع للمعالجة اليومية ، وفي نفس الوقت كالنسخة الأصلية.
- حيثما تتطلب حساسية المعلومات المحافظة على سريتها ، يجب إخضاع استعمالها لضوابط وشروط معينة ، وذلك بهدف حمايتها من المستعملين غير المصرّح لهم بذلك.

٣,٤,٥. البرامج التطبيقية

على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تتنبّه إلى الأمور التالية:

- يجب على برامج فحص هويّة المستعمل أن تعتمد على تعريفه كما ورد حين دخوله النظام ، وليس عبر أي تعريف بديل أو مستجد خلال مراحل العملية التي يقوم بها.
- يجب اعتماد مقاييس موحدة لتسمية التطبيقات والبرامج والملفات وقواعد المعلومات والعناصر أو الوحدات التي تؤلفها (Naming Convention).
- يجب أن تتوافق برامج آلية الدخول إلى النظام مع القواعد الموضوعة للمتطلبات والصلاحيات الممنوحة لمستعملي النظام.
- يجب فحص فعالية برامج الحماية (Application's Protective Mechanism) بعد كل تعديل على البرامج ، للتأكد من محافظتها على سلامة أداءها.

- يجب أن تتضمن البرامج عناصر لفحص شرعية وصحة المعلومات المدخلة
(Edit Routines, Range/Reasonableness Checks, Batch Totals, Sequence Number, Check Sums, Error Correcting Codes).
- يجب أن يلحظ النظام إمكانية ترميم نفسه آليا" ، بعد حوادث التوقف الطارئة (Automatic Recovery After System Crash).
- يجب أن تكون عملية نسخ المعلومات والبرامج ، شاملة ووافية لضمان نجاح ترميم النظام بعد حوادث التوقف الطارئة.
- يجب أن تحفظ عمليات المعالجة فورا" ، في أمكنة بعيدة نسبيا" عن مكان معالجتها (Offsite Location).
- يجب أن يتم قيد العمليات لمهمات المراقبة (Application Logs) في سجل خاص يتضمن المعلومات الوافية لاستعادة مقوّمات العمليات ومنفذيها.

٣,٥. البيئة المحيطة بالأجهزة

٣,٥,١. نظام أمان مراكز الأجهزة المعلوماتية:

من أجل تأمين الحماية اللازمة لأجهزة المعلوماتية والوسائط الممغنطة التي تحفظ عليها المعلومات الأساسية ، على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تراعي الأمور التالية:

٣,٥,١,١. في الترتيبات الإدارية

- عند اختيار موقع مركز الجهاز الأساسي ، على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تؤمن حماية هذا المركز من الحوادث الطبيعية، مثل حوادث السيول والطوافانات، والهزّات الأرضية ، والحريق ، الخ... واتخاذ التدابير والإجراءات اللازمة لمنع عمليات السرقة أو التخريب.
- عند اختيار جهاز بديل للجهاز الأساسي بغية الاستفادة منه في حالات الطوارئ وتوقّف الجهاز الأساسي، يجب وضع هذا الجهاز في منطقة جغرافية غير قريبة من الموقع الأساسي. أما كيفية اختيار هذا الموقع، فتخضع لاعتبارات وعوامل عدة.
- عند توزيع الأدوات المعلوماتية على كافة الأقسام والفروع ، يجب مراعاة موقع كل قطعة بشكل يمنع سرقة المعلومات... (مثلا" إبعاد شاشة الجهاز الأساسي عن النوافذ والممرّات).
- يجب أن يمنع دخول موظفي صيانة أجهزة المعلوماتية دون حضور أحد موظفي المؤسسة ، الملمّين بطبيعة عمل الصيانة والمخاطر المترتبة من جرائها.
- يجب حفظ الوسائط الممغنطة (Removable Media) في مستوعب مقفل، وإعطاء المفاتيح فقط للأشخاص المخولين الحصول عليها.

- وضع لوائح محددة بأسماء الأشخاص المصرّح لهم الدخول إلى مراكز أجهزة المعلوماتية ، مع تحديد دوام عملهم بدقّة.
- مسك سجل يومي لقيد أسماء الداخلين، وتاريخ الدخول، وساعة الدخول، وسبب الدخول ، وساعة الخروج ، وتواقيع الداخلين والخارجين من مراكز الأجهزة المعلوماتية ومراكز حفظ المعلومات الأساسية.
- يجب كتابة وتوثيق تدابير صيانة أجهزة المعلوماتية والأجهزة المحيطة (مثل أجهزة ضبط الطاقة (UPS) والتبريد والإطفاء والإنذار، الخ...) ، على أن تكون متوافقة مع تعليمات المصنّع في كيفية إجراء هذه الصيانة.
- وضع منهجية مفصلة لكيفية الإبلاغ عن أي عطل في الأجهزة المحيطة والإجراءات المتخذة لصيانة هذه الأجهزة.
- توثيق أعمال الصيانة الدورية والأعطال الطارئة وطرق معالجتها في سجل خاص، على أن تحفظ المعلومات المدوّنة فيه ، لفترة لا تقل عن سنتين من تاريخ حصولها.

٣,٥,١,٢.في الترتيبات التقنية

- تأمين شبكة وصل أرضي (System Grounding) خاضعة للمعايير العالمية، والتأكد من فعاليتها دوريا".
- تأمين التبريد المتواصل لضبط الحرارة ونسبة الرطوبة في مراكز أجهزة الكمبيوتر الأساسي.
- التأكد من أن النوافذ المستعملة للتبريد ، والتي تعطي إلى الخارج ، هي مقفلة ولا تسمح بإدخال أية أشياء من خلالها قد تسبب بتخريب الأجهزة المعلوماتية داخل المركز.
- تأمين أجهزة محيطة ، كأجهزة تبريد بديلة في حال توقف الأجهزة الأساسية.

- وضع الوسائط الممغنطة التي تحفظ عليها المعلومات يوميا" ودوريا" في مستوعبات خاصة ضد الحريق.
- وضع منهجية مفصّلة لكيفية تلف الوسائط الممغنطة:
  - طريقة التلف (حرق، تقطيع، تدمير، الخ...)
  - أمكنة حفظ الوسائط المطلوب إتلافها (بمنأى عن السرقة أو الإفادة غير المشروعة)
  - موعد تلفها
  - الموظف المسؤول عن عملية التلف.
- يجب تطبيق نفس قواعد الأمان المعمول بها في المركز الرئيسي ، على المراكز المعلوماتية الثانوية (Secondary and Alternate Sites) ، وعلى الأمكنة الخارجية (Off-Site Locations) لحفظ المعلومات.
- عند نقل الوسائط الممغنطة إلى خارج المؤسسة، يجب نقلها في مستوعب مقفل ، لا يمكن فتحه خلال عملية النقل ، ومحمي من تقلبات الحرارة والرطوبة.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تضع خطة مفصّلة لإخلاء مركز المعلوماتية في حالات الطوارئ ، تتناول كيفية تأمين حماية الموظفين ، ونقل أجهزة المعلوماتية والمعلومات الأساسية ، وظروف الإخلاء، والخطوات الواجب اتخاذها قبل الإخلاء ، كوضع الموظفين في أجواء الخطة وتدريبهم عليها.

٣,٦. العمليات

٣,٦,١ في إدارة العمليات

- إن القيّمين على العمليات في استعمال النظام ، هم كافة العاملون على أدوات النظام (الجهاز الرئيسي ، والأجهزة الثانوية ، والشبكات ، ومحطات الإدخال)
(Main-Frames, Mini-Computers, Networks and Workstations).
- يجب ألا يتمتع مسئولو العمليات ، بأية إمكانية لتعديل البرامج المنفّذة أو مناهج تنفيذها (Executable Programs or Initiations Procedures).
- يجب تشغيل الأجهزة المستعملة في بيئة العمليات ، بواسطة العاملين المصرّح لهم بذلك فقط.
- يجب تطبيق مبدأ التبديل الدوري للعاملين في العمليات ، بهدف المراقبة والتدقيق (Rotation of Operators on Sensitive Applications).

٣,٦,٢ في الموافقة على استعمال النظام

- يجب أن تشمل موافقات الاستعمال كل نوع من أنواع العمليات
(Authorizations For all Types of Operations)
- يجب أن تحفظ الموافقات على وسائط ممغنطة ، وعلى عدة نسخ ، بشكل يمكّن من مراجعتها بسهولة ، خاصة" إذا لم يتمّ توثيقها وحفظها على المطبوعات الورقية.
- يجب ألا يتمكن العاملون في العمليات ، من الدخول على أنظمة وعناصر تكنولوجيا المعلومات المختلفة والخارجة عن نطاق صلاحياتهم
(No Access to IT Systems).

- يجب تعريف المستعمل ضمن مجموعة تحمل نفس الصلاحيات ، بشكل توضح هويته دون أي التباس (Users of the Same Group).
- عند استعمال رموز التعريف وكلمات السرّ ، يجب تأكيد الأمور التالية:
  - إن آلية إصدار وإدارة وتوزيع كلمات السرّ تراعي مبدأ سريتها وسلامتها
  - لا تعرف كلمات السرّ إلا من العامل المعني باستعمالها فقط
    - من دواعي الأمان أن تُلحظ برامج متخصصة لرصد إعادة استعمال نفس كلمات السر لأكثر من فترة ، أو لكلمات مبسطة جدا" حيث يسهل بالتالي ، استنتاجها
    - يجب ألا تقلّ كلمات السر عن الستة أحرف (Alphanumerical)
    - يجب وضع آلية تفرض تغيير كلمات السر دوريا" على ألا تتعدى الشهرين على الأكثر ، والشهر الواحد للحالات الحساسة.
    - يجب أن تتمّ عمليةّ تشفير كلمات السر ، بوسيلة واحدة وفريدة (One-Way Encryption Method)
- يجب أن يتم قيد تعريف المستعملين، عند قيامهم بعملهم، بسجل خاص ذي درجة حساسية عالية ، ويوثّق ويحفظ على هذا الأساس.

٣,٦,٣. في أمور العمليات اليومية ومراقبتها

- يجب أن تلحظ قواعد تنظيم العمليات اليومية الأمور التالية:

- Power up/Power down sequence,
- Start up/Shut down of systems (including operating system and applications),
- Equipment operation,
- Trouble reporting,
- Security incident handling,
- Operator-performed maintenance,
- Operator commands,
- Operator responses to systems and application program-generated messages,
- Start and stop communications,
- Backup
- Restore (must be approved and controlled by authorized personnel),
- Sanitizing erasable media,
- Disposal of unserviceable erasable media,
- Emergency situations,
- Shift hand-over,
- Over-riding of security controls,
- Recovery/restart,
- Environmental support equipment,
- Setting and resetting the system clock.

- يجب أن يسبق عملية قبول النظام ، والذي يتطلب موافقة المستعملين عليه، تدريب هؤلاء على استعماله ، وتوفير مستندات كل قواعد العمليات التي يحتويها.
- يجب أن تتمّ عملية تدقيق العمليات اليومية بواسطة فريق مختلف عن الذي يقوم بعملية الإدخال.
- يجب وضع التدابير اللازمة للتأكّد من حسن تنفيذ أعمال حفظ ونسخ الملفات وقواعد المعلومات (For Ensured Successful Back-Ups).
- يجب حفظ عدد نسخ كافية عن الملفات وقواعد المعلومات ، لضمان نجاح عملية ترميمها بعد الحوادث الطارئة (Ensure recovery of Data).

- يجب وضع تعليمات وتدابير لكيفية انتقال إدارة العمليات على الأجهزة أو البرامج ، من فريق إلى فريق آخر ، أو إلى موظفي الصيانة ، على ألا يمسّ هذا الانتقال بقواعد الأمان المتبعة.
- يجب عدم تجاوز التعريف الآلي لوسائط المعلومات (Override Machine Readable Labels) ، عند قراءتها من قبل البرامج المعالجة ، إلا عبر موافقة مكتوبة بذلك.
- وفي حال تجاوز التعريف الآلي لوسائط المعلومات ، يجب وضع آلية للتأكد من استعمال الوسائط الصحيحة (Correct Volume Is Mounted).

٣,٦,٤ ضبط تبادل المعلومات (Input-Output Controls)

- لا يتمّ إصدار إلا العدد المسموح به فقط من التقارير المطلوبة.
- إن إعادة إصدار التقارير والمعلومات ، يجب أن تتمّ بموافقة خطية مسبقة من الجهة المصرّح لها بذلك.
- يجب أن تسلّم التقارير إلى طالبها فقط ، أو من هو مكلّف رسميا" من قبله، بواسطة آلية تسلّم واستلام خطيّة وموقّعة.
- إن إرسال التقارير والمعلومات عن بعد ، يجب ألا يسمح بالإطلاع عليها من قبل جهات غير مصرّح لها بذلك.

٣,٦,٥. في التدقيق والرقابة على العمليات

- على العاملين في العمليات ، أن يوقّعوا على سجل خاص عند بدئهم بالأعمال المعهودة إليهم ، وعند انتهاءهم منها.
- يجب أن يصدر عن النظام تقارير ، ترصد استعمالاته ، مع تفصيل الأخطاء الواقعة ونسبة تكرارها.

- يجب التدقيق بأوقات متفرّقة ، بالتقارير الصادرة عن النظام حول استعمالاته المختلفة (System Logs) ، للتأكد أن كل الأعمال المنفذة حائزة على الموافقة المطلوبة.
- يجب تسمية المسؤولين عن الوسائط المنقولة لحفظ المعلومات (Removable Media) ، مع تحديد مسؤولياتهم ومهامهم.

٣,٧.في إدارة خزانة الوسائط المنقولة للمعلومات (Removable Media)

- يجب أن تكون إدارة خزانة الوسائط المنقولة ، بعهدة الموظفين المصرّح لهم بذلك فقط ، وأن تكون موثّقة ومراقبة.
- يجب حماية هذه الوسائط المنقولة (Removable Media) عند انتزاعها من أجهزتها، (When Removed From The Drive) وجعلها غير قابلة للتعديل أو الكتابة (Write-Protection Enabled).
- باستثناء الأعمال اليومية والدورية الروتينية التي تتعلق باستعمال الوسائط المنقولة والتي تخضع لموافقة صريحة مسبقة ، يجب عدم إتاحة إمكانية التعديل أو الكتابة على الوسائط المنقولة (Enabling Write-Protection) إلا بواسطة المسؤولين المصرّح لهم بذلك.
- عند حفظ هذه الوسائط خارج المؤسسة (Off-Site Location) ، يجب التأكد من أن هذا المكان يراعي قواعد الأمان الضرورية.
- يجب إعلام المسؤول عن أمان تكنولوجيا المعلومات فورا" ، عن كل سوء استعمال للوسائط المنقولة.

- عند نقل الوسائط إلى مكان حفظها خارج المؤسسة (Off-Site Location) ، يجب توضيبها بشكل يمنع قراءتها أو استعمالها.
- يجب أن تتمّ جردة الوسائط المنقولة ، بواسطة شخصين أو أكثر معا" ، على أن يكون أحدهم من غير الموظفين المسؤولين عنها.
- يجب التدقيق الميداني ، من وقت إلى آخر ، في محتويات خزانة الوسائط المنقولة ومقارنتها مع المعلومات المدوّنة في الدفاتر اليومية.
- يجب أن تحتوي هذه الوسائط على تعريف داخلي (Machine Readable Internal Labels) ، كما يجب وضع آلية للتأكد من وجود التعريف الداخلي فيها.
- على النظام أن يقرأ تعريف هذه الوسائط حين وضعها داخل الأجهزة ، والتأكد منها قبل استعمالها.
- يجب التأكد من محو الوسائط المنقولة كليا" قبل إتلافها أو تغيير وجهة استعمالها، وأن تتمّ هذه العملية بعد موافقة الجهة المخوّلة السماح بها.

٣,٨. منهجية شراء أو تطوير الأنظمة المعلوماتية

إن اتباع منهجية واضحة في عملية اختيار وتطوير مواد تكنولوجيا المعلومات، يمكّن المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية من تفادي مشاكل محتملة تنتج عادة" عن الإهمال في دراسة وافية للاحتياجات الفعلية للمؤسسة أو عن سوء اختيار لمورّد هذه المواد. لذا فمن الضروري إيلاء الأمور الأساسية التالية الاهتمام الكافي قبل الاختيار:

- تحديد أهداف عملية التحديث أو التطوير.
- تحديد الاحتياجات بطريقة شاملة وبشكل يتلاءم والتوجهات العامة للسوق، وبالتعاون مع كل المعنيين من إداريين وتقنيين والمستعملين المحتملين لهذه المواد.
- وضع دفتر المواصفات لاستقبال العروض (REQUEST FOR PROPOSAL (RFP)) ، وتضمينه إضافة" إلى المتطلبات والمواصفات العملية كافة" (SYSTEM FUNCTIONALITY)، متطلبات الجودة وشروطها (QUALITY PERFORMANCE).
- وضع لائحة بالمورّدين المؤهلين بتقديم هذه المواد.
- اختيار الأنسب بين هذه العروض بالارتكاز على المؤشرات التالية:
  ١. مدى تطابق العرض مع المواصفات المطلوبة (PRODUCT VERSUS SYSTEM REQUIREMENTS)
  ٢. خبرة وإنجازات المورد (VENDOR OR SUPPLIER REFERENCES)
  ٣. استمرارية خدمات المورد واستقرار وضعه المالي (VENDOR VIABILITY / FINANCIAL STABILITY)
  ٤. استعداد المورد إلى تقديم كامل مستندات النظام
  ٥. مستوى الصيانة والدعم لدى المورد (VENDOR SUPPORT)

٦. عدد سنين الخبرة الفعلية للنظام المطلوب
٧. استلام البرامج الأساسية (SOURCE PROGRAMS) أو الاتفاق مسبقا" على إيداع عدة نسخ منها في أماكن أمينة وجاهزة للاستعمال في حالات معيّنة ، كتوقّف خدمات المورد لسبب ما
٨. الاتفاق على الشروط العامة الأساسية ، مثل مدة إنجاز النظام ، الطاقم المهيّأ لاختباره وإقرار جدارته قبل عملية قبوله

- من الضروري توثيق كل الدراسات والتطورات المتعلقة بهذا الموضوع ضمن ملفات ومحاضر جلسات الفريق المخوّل البتّ به.

٣,٩. خطط الطوارئ ومعاودة العمل

إن خطط الطوارئ لها أهمية كبرى في ضمان سلامة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية في كل الظروف وفي ضمان استمرارية عملها في الحالات الطارئة. والتوصّل إلى وضع هذه الخطط يخضع لدراسة مستفيضة حول كيفية استمرار خدمات المؤسسة، خاصة" الحساسة منها، دون أي توقّف أو تعثّر، ممّا يفرض وضع الحلول المناسبة للتصدّي لعدة سيناريوهات من المشاكل والحوادث الممكنة. وبعد اعتماد هذه الحلول ، يجب توفير الإمكانيات التي تتطلّبها بصورة مستمرة وتأمين الشروط لحسن تطبيقها ، كما يجب توثيقها واختبارها فعليا" وتدريب الموظفين عليها ومراجعتها دوريا" للتأكد من استمرار فعاليتها بكل الظروف خاصة" المتغيّرة منها.

- لذا فعلى كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية أن تحدد في دراستها لحساسية أدوات المعلوماتية وعملياتها العناصر التالية:
  - سقف الخدمات الحساسة والضرورية.
  - الفترة القصوى لتوقف النظام المعلوماتي أو الأجهزة.
  - متطلبات عملية نسخ المعلومات الدورية، لأهميتها في إعادة الانطلاق من المعلومات الصحيحة في الحالات الطارئة.
  - الاحتياط للحالات الطارئة ووضع الحلول لها ومن أهم هذه الحالات:
    - المعالجة نتيجة عطل في الأجهزة والنظام
    - استمرار الخدمات الحساسة إثر تدمير كلي لمصدرها الأساسي
    - الاضطرابات العامة
    - تخلّف أحد الموردين عن إسداء الخدمات المطلوبة
    - تخلّف أو توقّف بعض العناصر البشرية داخل المؤسسة عن تسيير إحدى الخدمات المسؤولين عنها.

- على خطط الطوارئ هذه ألا تعطّل قواعد الأمان المرعية وألا تؤثر عليها، مهما كانت الظروف.
- يجب حفظ أكثر من نسخة عن هذه الخطط وتدابير الطوارئ ، في أمكنة متباعدة جغرافيا".
- يجب أن يتوفّر في المؤسسة ، العناصر البشرية المدرّبة على خطط الطوارئ وكذلك العناصر البديلة لها، حفاظا" على استمرارية الخدمات الحساسة ، وأن يتمّ تدريبها نظريا" وعمليا" على القيام بالعمل المطلوب ، بكل ثقة وأمان.
- على كل مصرف أو مؤسسة مالية أو مؤسسة وساطة مالية، ونتيجة لدراسة تقييمية لحجم مخاطر تكنولوجيا المعلومات لديها، أن تلجأ إلى عقود التأمين لتغطية أية خسارة قد تنتج عن المشاكل والحوادث التي تفوق نطاق المعالجات الذاتية الأكيدة.

٤. الفترة الزمنية لتطبيق قواعد أمان تكنولوجيا المعلومات

إن تطبيق قواعد أمان تكنولوجيا المعلومات المذكورة في هذا الكتيّب ، يتطلّب جهودا" كبيرة ومتواصلة ، من جانب المصارف والمؤسسات المالية ومؤسسات الوساطة المالية ، تبدأ بتشكيل لجان عمل ، تضمّ اختصاصيين بأمور الإدارة والعمليات وتكنولوجيا المعلومات والمدققين ، فضلا" عن ممثلين عن الإدارة العليا في المؤسسة. وقد تستعين هذه اللجان في بعض الحالات، بأخصائيين من الخارج ، لتعميق البحث في بعض مواضيع الأمان والحلول المطروحة. ولا شك أن إرساء القواعد السليمة للعمل ، هو مسؤولية مشتركة بين كل أفرقاء القطاع المصرفي والمالي ، وأن اعتماد مقاييس عالمية لأمور تكنولوجيا المعلومات، يساعد على تركيز لغة تكنولوجيا مشتركة للبنان ، سيكون لها الصدى الإيجابي لدى المؤسسات العالمية.

لذا يجب إعطاء الفترة الزمنية المحددة للقيام بالجهود المطلوبة ، لإرساء هذه القواعد والتي قد تتراوح من عدة أشهر للمؤسسات المهيأة للتطبيق السريع ، إلى أكثر من سنة في حال إعادة هندسة العمل جذريا".

لكن لا بدّ من التقدّم نحو أهداف التوجيهات عبر مراحل متتالية، يتمّ خلالها تطبيق قواعد الأمان تباعا" حتى تكتمل كل شروطها وعناصرها. أما هذه المراحل ، فهي تمتدّ على ثلاث فترات ، تتوزّع خلالها الجهود بحسب الجدول رقم (٤,١) المرفق.

إن لجنة الرقابة على المصارف ستزوّد المصارف والمؤسسات المالية ومؤسسات الوساطة المالية المعنية كافة" ، وقبل انتهاء كل مرحلة من المراحل الثلاث ، بالاستمارة التي تبيّن ، بعد تعبئتها من قبلها ، مدى تقدّمها في تطبيق قواعد الأمان المطلوبة.