

نهاد ریاست جمهوری - وزارت امور اقتصادی و دارایی
بانک مرکزی جمهوری اسلامی ایران

هیئت وزیران در جلسه ۱۴۰۵/۳/۱۰ به پیشنهاد شورای ملی تأمین مالی (موضوع نامه شماره ۸۰/۱۶۹۵۵۴ مورخ ۱۴۰۴/۹/۱۵ وزارت امور اقتصادی و دارایی) و به استناد اصل یکصد و سی و هشتم قانون اساسی جمهوری اسلامی ایران و جزء (۳-۵-۳) بند (ب) ماده (۲) و بند (ب) ماده (۴۶) قانون تأمین مالی تولید و زیرساختها مصوب ۱۴۰۲، آیین نامه اجرایی جزء یادشده را به شرح زیر تصویب کرد:

آیین نامه اجرایی جزء (۳-۵-۳) بند (ب) ماده (۲) قانون تأمین مالی تولید و زیرساختها
(موضوع حفاظت اطلاعات و حفظ محرمانگی و امنیت داده های شرکت های اعتبارسنجی)

- ماده ۱- در این آیین نامه، اصطلاحات زیر در معانی مشروح مربوط به کار می روند:
- ۱- قانون: قانون تأمین مالی تولید و زیرساختها مصوب ۱۴۰۲ با اصلاحات بعدی
 - ۲- شورا: شورای ملی تأمین مالی موضوع بند (الف) ماده (۲) قانون
 - ۳- بانک مرکزی: بانک مرکزی جمهوری اسلامی ایران
 - ۴- مرکز: مرکز ملی تأمین مالی وزارت امور اقتصادی و دارایی
 - ۵- مرکز افتا: مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست جمهوری
 - ۶- پایگاه داده اعتباری: پایگاه داده اعتباری کشور، موضوع تبصره (۴) بند (ب) ماده (۲) قانون
 - ۷- آیین نامه تأسیس: آیین نامه نحوه تأسیس و فعالیت شرکت های اعتبارسنجی موضوع جزء (۱-۵-۳) بند (ب) ماده (۲) قانون موضوع تصویب نامه شماره ۱۶۸۹۰۹/ت/۶۳۳۷۹ مورخ ۱۴۰۳/۱/۳
 - ۸- اطلاعات مکمل: موضوع بند (۹) ماده (۱) آیین نامه تأسیس
 - ۹- امتیاز اعتباری: موضوع بند (۱۲) ماده (۱) آیین نامه تأسیس
 - ۱۰- گزارش اعتباری: موضوع بند (۱۳) ماده (۱) آیین نامه تأسیس
 - ۱۱- شرکت: شرکت های اعتبارسنجی نوع یک موضوع بند (۱۵) ماده (۱) آیین نامه تأسیس و شرکت های اعتبارسنجی موضوع بند (۱۶) ماده (۱) آیین نامه تأسیس که دارای مجوز فعالیت ارائه خدمات بند (۱) و (۴) ماده (۲۰) آیین نامه تأسیس هستند.



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره ۲۹۹۹۳
تاریخ ۱۳۹۰/۵/۱۴
تاریخ ۱۴۰۵/۳/۳۱

ماده ۳۳- شرکت های موجود فعال در زمینه اعتبارسنجی موظفند برنامه های راهبردی خود را به گونه ای تنظیم کنند تا ظرف یک سال پس از ابلاغ این آیین نامه، نرم افزارهای مورد استفاده خود را بومی سازی نموده و منضم به گزارش مدیریت تطبیق و امنیت اطلاعات، جهت تأیید به مقام ناظر بر فرایند تأمین امنیت ارائه کنند.

ماده ۳۴- مسئولیت اجرای مفاد این آیین نامه با مدیران شرکت ها بوده و مدیریت تطبیق و امنیت اطلاعات صرفاً موظف به پایش، ارزیابی، گزارش دهی و اطلاع رسانی به مقام ناظر بر فرایند تأمین امنیت است. مدیریت مذکور نباید در امور اجرایی شرکت ورود یا خللی ایجاد نماید.

ماده ۳۵- افراد موضوع این آیین نامه در صورت تخلفی از مفاد این آیین نامه، مشمول مقررات انتظامی آیین نامه اعمال مقررات انتظامی متناسب با تخلفات شرکت های اعتبارسنجی و مدیران آنها موضوع تصویب نامه شماره ۱۹۲۴۴۷/ت/۶۵۲۳۴ هـ مورخ ۱۴۰۴/۱۱/۲۱ هستند.

ماده ۳۶- مواد (۶)، (۱۰)، (۱۵)، (۱۶) و (۲۵) آیین نامه نظام سنجش اعتبار موضوع تصویب نامه شماره ۳۹۱۵۱/ت/۵۵۲۹۶ هـ مورخ ۱۳۹۸/۴/۴ لغو می گردد.

محمد رضا عارف
معاون اول رئیس جمهور

رونوشت به دفتر مقام معظم رهبری، دفتر رئیس جمهور، دفتر رئیس مجلس شورای اسلامی، دفتر رئیس قوه قضاییه، دفتر معاون اول رئیس جمهور، دبیرخانه مجمع تشخیص مصلحت نظام، دبیرخانه ستاد کل نیروهای مسلح، دیوان محاسبات کشور، دیوان عدالت اداری، سازمان بازرسی کل کشور، معاونت های قوانین و نظارت مجلس شورای اسلامی، امور تدوین، تنقیح و انتشار قوانین و مقررات، کلیه وزارتخانه ها، سازمان ها و مؤسسات دولتی، معاونت های رئیس جمهور، نهادهای انقلاب اسلامی، روزنامه رسمی جمهوری اسلامی ایران، دبیرخانه شورای اطلاع رسانی دولت و دفتر هیئت دولت.



جمهوری اسلامی ایران

رئیس جمهور

نصوب به هیئت وزیران

شماره ۲۹۹۹۳
تاریخ ۱۳۹۰/۵/۳۱
مخبر

- ۱۲- استفاده کنندگان: موضوع بند (۱۷) ماده (۱) آیین نامه تأسیس
- ۱۳- مشتری: موضوع بند (۱۸) ماده (۱) آیین نامه تأسیس
- ۱۴- تأمین کنندگان اطلاعات: موضوع بند (۲۰) ماده (۱) آیین نامه تأسیس و همچنین تأمین کنندگان اطلاعات مکمل
- ۱۵- مقام ناظر بر فرایند تأمین امنیت: شخص حقوقی که مسئولیت نظارت بر فرایند تأمین امنیت اطلاعات و سامانه های شرکت ها را بر عهده داشته و به شرح زیر است:
 - الف- شرکت های تحت نظارت بانک مرکزی: بانک مرکزی جمهوری اسلامی ایران
 - ب- شرکت های خارج از نظارت بانک مرکزی: وزارت امور اقتصادی و دارایی
- ۱۶- مدیریت تطبیق و امنیت اطلاعات: واحدی در شرکت ها جهت پیگیری و انجام وظایف مندرج در این آیین نامه.
- ۱۷- تصفیه اطلاعات: فرایند اصلاح، استانداردسازی و بهینه سازی داده های دریافتی از تأمین کنندگان اطلاعات که از دقت، یکپارچگی و قابلیت اطمینان داده های بارگذاری شده در سامانه شرکت اطمینان حاصل شود. این فرایند شامل شناسایی و رفع خطاها، ناسازگاری ها و نقص های موجود در داده های خام است، به نحوی که برای ذخیره سازی اطلاعات اعتباری و تهیه گزارش از اطلاعات دریافتی مقدور باشد.
- ۱۸- مجوز افتا: پروانه فعالیت در حوزه افتا (گواهی مرکز افتا) که توسط مرکز افتا برای شرکت ها صادر می شود.
- ۱۹- طرح بازیابی از فاجعه: طرحی که در صورت بروز حوادث قهری اعم از زلزله، سیل و طغیان های غیرعادی، آتش سوزی های دامن دار و مهارنشدنی، طوفان، شیوع بیماری های واگیردار و حوادث مشابه خارج از مهار (کنترل)، امکان ارائه خدمات (سرویس) توسط شرکت را مختل می نماید به کمک آن می توان دسترسی پذیری و امنیت داده را تضمین نمود.
- ۲۰- طرح تداوم کسب و کار: مجموعه ای از فرایندها و دستورالعمل ها و اقدامات اجرایی که توسط شرکت با هدف بازیابی و ادامه روند فعالیت های جاری کسب و کار انجام و پیاده سازی می شود تا بتواند بعد یا در هنگام بروز حوادث قهری به روند فعالیت جاری خود ادامه دهد.
- ۲۱- توافق نامه همگاری: توافق نامه ای که بین شرکت ها با تأمین کنندگان اطلاعات یا استفاده کنندگان بر مبنای توافق نامه نمونه ای که توسط مقام ناظر بر فرایند تأمین امنیت ابلاغ می شود، منعقد می گردد و در آن جزئیات مربوط به حقوق، تعهدات و مسئولیت های هر یک از طرفین و نحوه تبادل اطلاعات و خدمات بین آنها به طور شفاف تبیین می شود.
- ۲۲- مدیران شرکت: مدیرعامل و اعضای هیئت مدیره شرکت ها.



جمهوری اسلامی ایران

رئیس جمهور

نصوب نامه هیئت وزیران

شماره ۲۹۹۹۳
تاریخ ۱۳۹۰/۵/۱۴
شماره ۱۴۰۵ / ۳ / ۳۱

ماده ۲- مسئولیت تأمین امنیت پایگاه داده اعتباری مطابق ضوابط اعلامی مرکز افتا و سایر مراجع قانونی ذی ربط، بر عهده بانک مرکزی خواهد بود. سازوکار تأمین امنیت پایگاه داده اعتباری مطابق دستورالعملی خواهد بود که ظرف یک ماه پس از ابلاغ این آیین نامه، توسط بانک مرکزی با همکاری مرکز افتا تدوین و توسط بانک مرکزی ابلاغ می گردد. دستورالعمل مذکور باید مشتمل بر الزامات ناظر بر جلوگیری از سوءاستفاده واسطه های دسترسی به داده به منظور جلوگیری از انباشت اطلاعات پایگاه داده اعتباری نزد شرکت ها و استفاده کنندگان باشد.

تبصره ۱- نمایندگان وزارت امور اقتصادی و دارایی، بانک مرکزی و سایر اشخاصی که در انجام فعالیت خود به داده ها و اطلاعات مشتری نزد پایگاه داده اعتباری دسترسی پیدا می کنند، موظفند با رعایت اصل امانت داری، رازداری و محرمانگی، داده ها و اطلاعات مذکور را به عنوان اسرار حرفه ای تلقی نموده و از افشای آن خودداری نمایند و در غیر این صورت، برابر قوانین و مقررات مربوط، از جمله قانون جرایم رایانه ای مصوب ۱۳۸۸ با اصلاحات بعدی با آنها رفتار خواهد شد. افرادی که به داده ها و اطلاعات پایگاه داده اعتباری دسترسی پیدا کنند، لازم است قبل از دسترسی به داده ها و اطلاعات، صلاحیت عمومی آنان به تأیید حراست بانک مرکزی رسیده باشد.

تبصره ۲- استفاده از پیمانکاران و مشاوران خارجی برای طراحی، معماری و پیاده سازی پایگاه داده اعتباری توسط بانک مرکزی یا شرکت های تابعه و وابسته به آن بانک، تحت عنوان قراردادهای مشاوره یا هر عنوان دیگر ممنوع بوده و بانک مرکزی می تواند از شرکت های داخلی که تأییدیه صلاحیت آنها از حراست بانک مرکزی دریافت شده باشد، برای تحلیل، معماری و پیاده سازی پایگاه داده اعتباری استفاده نماید.

ماده ۳- به منظور بررسی و تأمین امنیت سامانه ها، نرم افزارها، پایگاه داده داخلی و داده ها و اطلاعات شرکت ها، هر یک از این شرکت ها مکلف به ایجاد واحد تخصصی مدیریت تطبیق و امنیت اطلاعات هستند. این واحد موظف به پیگیری و اجرایی کردن الزامات این آیین نامه و تضمین امنیت داده ها و اطلاعات و انطباق با استانداردهای مرتبط می باشد.

ماده ۴- شرکت ها باید نسبت به پیشنهاد مدیر واحد تطبیق و امنیت اطلاعات به مقام ناظر بر فرایند تأمین امنیت اقدام نموده و تأییدیه لازم را از آن مقام اخذ نمایند. انتصاب مدیر تطبیق و امنیت اطلاعات باید با رعایت معیارهای تخصصی امنیت داده ها، تطبیق مقررات و مدیریت خطر (ریسک) فناوری اطلاعات با تشخیص مقام ناظر صورت پذیرد.

تبصره ۱- مقام ناظر بر فرایند تأمین امنیت موظف است پیش از ارائه تأییدیه، نسبت به اخذ استعلام از مرکز افتا اقدام نماید. مرکز افتا نیز موظف است حداکثر ظرف یک ماه پس دریافت درخواست از سمت مقام ناظر بر فرایند تأمین امنیت، نسبت به پاسخ به درخواست واصله اقدام نماید. عدم ارائه پاسخ ظرف مهلت مشخص شده، به منزله تأیید مرکز افتا خواهد بود.



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره
تاریخ
۱۳۰۵ / ۳ / ۳۱

تبصره ۲- هرگونه استعفاء، جابجایی یا تغییر در مدیریت تطبیق و امنیت اطلاعات منوط به تأیید مقام ناظر بر فرایند تأمین امنیت خواهد بود. در صورت استعفاء یا جابجایی مدیر، تا معرفی مدیریت جدید، مدیریت فعلی به فعالیت خود ادامه خواهد داد.

تبصره ۳- در صورت عزل یا قوت مدیریت تطبیق و امنیت اطلاعات، مدیرعامل شرکت موظف است ظرف یک هفته گزینه پیشنهادی خود را به مقام ناظر بر فرایند تأمین امنیت معرفی نماید. بدیهی است که در این حالت تا معرفی و تأیید مدیریت جدید، مسئولیت مستقیم عملکرد مدیریت تطبیق و امنیت اطلاعات با مدیرعامل شرکت خواهد بود.

ماده ۵- مدیران شرکتها موظفند هرگونه تغییر در فرایندهایی از شرکت را که به گونه‌ای با اطلاعات و داده‌های شرکت مرتبط است، به اطلاع مدیریت تطبیق و امنیت اطلاعات برسانند.

ماده ۶- مدیران شرکتها موظفند کلیه الزامات و دستورالعمل‌های صادره توسط مدیریت تطبیق و امنیت اطلاعات را به شکل کامل رعایت نموده و هماهنگی لازم را برای اجرای مؤثر آنها به عمل آورند. همچنین، مسئولیت ارتقای سطح آگاهی و توانمندسازی نیروی انسانی در حوزه امنیت داده‌ها بر عهده مدیران شرکتها است.

ماده ۷- با هدف نظارت دقیق و کامل بر استفاده از داده‌ها و اطلاعات دریافتی از تأمین‌کنندگان داده‌ها و اطلاعات، مدیران شرکتها موظفند دسترسی مدیریت تطبیق و امنیت اطلاعات به داده‌های زیر را در سامانه‌ها و نرم‌افزارهای شرکت فراهم نمایند:

- ۱- رویدادنگاری (لاگ) انواع تغییرات در داده‌ها و اطلاعات پایگاه داده داخلی شرکت.
- ۲- رویدادنگاری (لاگ) کلیه استعلام‌های گزارش اعتباری و یا سایر محصولات و خدمات اعتباری ارائه‌شده توسط شرکت.

۳- سایر داده‌ها و اطلاعات و مستندات مربوط به امنیت داده به تشخیص مدیریت تطبیق و امنیت اطلاعات.

ماده ۸- در صورتی که خاتمه فرایند رسیدگی به اعتراض بر اساس آیین‌نامه موضوع جزء (۵-۳) بند (ب) ماده (۲) قانون موضوع تصویب‌نامه شماره ۴۶۴۳۵/ت ۴۱۷۲ هـ مورخ ۱۴۰۴/۳/۱۷، به اصلاح داده‌ها و اطلاعات منجر شود، سامانه‌ها و نرم‌افزارهای تخصصی شرکتها باید به نحوی پیاده‌سازی شوند که به تفکیک، رویدادنگاری (لاگ) تغییرات مذکور را ذخیره نمایند.

ماده ۹- مدیران شرکت‌های اعتبارسنجی موظفند برای سامانه‌های تحت اختیار خود و همچنین تجهیزات ذخیره اطلاعات، مجوزهای امنیتی از مرکز افتا، بررسی‌های امنیتی و تست نفوذ توسط شرکت‌های دارای مجوز افتا را تهیه کرده و به تأیید مدیریت تطبیق و امنیت اطلاعات برسانند.

تبصره ۱- مدیران شرکت‌های اعتبارسنجی موظفند گواهینامه استاندارد سامانه (سیستم) مدیریت امنیت اطلاعات را از شرکت‌های دارای مجوز از مرکز افتا، جهت پیاده‌سازی فرایندها و رویه‌های داخلی شرکت خود دریافت نمایند.



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره
تاریخ
۱۳۰۵ / ۳ / ۳۱

تبصره ۲- هرگونه به روزرسانی یا توسعه در سامانه ها و نرم افزارهای تخصصی شرکت ها به نحوی که منجر به تغییر در ذخیره سازی داده ها و اطلاعات و رویدادنگاری های (لاگ) مندرج در ماده (۷) این آیین نامه گردد، باید به تأیید مدیریت تطبیق و امنیت اطلاعات برسد.

ماده ۱۰- مدیران شرکت ها در خصوص زیرساخت های فناوری اطلاعات مورد استفاده، ملزم به رعایت استانداردهای مرتبط با مراکز داده و مورد تأیید مقام ناظر بر فرایند تأمین امنیت هستند.

ماده ۱۱- مدیران شرکت ها موظفند طرح بازیابی از فاجعه و طرح تداوم کسب و کار را مطابق ضوابط اعلام شده توسط مقام ناظر بر فرایند تأمین امنیت، برای سامانه های اعتبارسنجی و تجهیزات ذخیره سازی داده ها و اطلاعات تهیه و اجرا نمایند. مدیریت تطبیق و امنیت اطلاعات موظف است به صورت دورهای و بنا به درخواست، گزارش عملکرد این حوزه را به مقام ناظر بر فرایند تأمین امنیت ارائه نمایند.

ماده ۱۲- مدیریت تطبیق و امنیت اطلاعات موظف است به صورت مستمر و با استفاده از داده ها و اطلاعات موضوع ماده (۷) این آیین نامه و فرایندها و قواعد موضوع ماده (۵) این آیین نامه، موارد مشکوک به تغییر یا ایجاد دسترسی غیرمجاز در سامانه ها، نرم افزارهای تخصصی و داده ها و اطلاعات شرکت ها را استخراج نموده و به همراه مستندات به مدیرعامل ارائه نماید. مدیرعامل شرکت موظف است ظرف هفت روز کاری، دلایل مبنی بر پذیرش تغییر یا دسترسی غیرمجاز را به مدیریت تطبیق و امنیت اطلاعات گزارش نماید. در صورت عدم گزارش دلایل یا عدم کفایت ادله گزارش شده توسط مدیرعامل شرکت ظرف مهلت زمانی مقرر، مراتب توسط مدیریت تطبیق و امنیت اطلاعات به مقام ناظر بر فرایند تأمین امنیت گزارش خواهد شد. پس از آن، مقام ناظر بر فرایند تأمین امنیت نسبت به ارائه گزارش تغییرات یا دسترسی های غیرمجاز به سامانه ها، نرم افزارهای تخصصی و داده ها و اطلاعات شرکت ها به شورا اقدام خواهد نمود. شورا با توجه به سطح اهمیت تغییرات یا دسترسی های غیرمجاز، یک یا چند مورد از اقدامات نظارتی موضوع جزء (۲-۵-۳) بند (ب) ماده (۲) قانون را در خصوص شرکت اتخاذ خواهد نمود.

ماده ۱۳- مسئولیت تأمین، حفظ و ارتقاء امنیت سامانه ها، نرم افزارها و پایگاه های داده داخلی و داده ها و اطلاعات شرکت ها بر عهده مدیران هر شرکت است.

ماده ۱۴- هر یک از اشخاصی که به اطلاعات و داده های شرکت ها دسترسی دارند، باید از حیث صلاحیت های عمومی به تأیید مقام ناظر بر فرایند تأمین امنیت برسند.

تبصره ۱- تشخیص مصادیق و معرفی اشخاص یا سمت هایی که به داده ها و اطلاعات و پایگاه داده داخلی شرکت ها دسترسی دارند، به عهده مدیریت تطبیق و امنیت اطلاعات خواهد بود.

تبصره ۲- اشخاص موضوع این ماده موظفند کلیه داده ها و اطلاعات و گزارش های اعتباری مشتری را محرمانه و به عنوان «اسرار محرمانه» تلقی نموده و از افشای آن خودداری نمایند. مدیر واحد تطبیق و امنیت اطلاعات موظف است الزامات و سازوکار لازم به منظور جلوگیری از افشای داده ها و اطلاعات را به مدیران



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره
تاریخ
تاریخ ۱۳۰۵ / ۳ / ۳۱

شرکت‌ها جهت اتخاذ تصمیم پیشنهاد نمایند. مدیران شرکت‌ها موظفند سازوکار لازم به منظور عقد تفاهنامه عدم افشاء را فراهم و به تأیید مدیریت تطبیق و امنیت اطلاعات برسانند.

تبصره ۳- اشخاص موضوع این ماده موظفند نسبت به عقد تفاهنامه عدم افشاء مورد تأیید مقام ناظر بر فرایند تأمین امنیت اقدام نمایند.

ماده ۱۵- نمایندگان مقام ناظر بر فرایند تأمین امنیت، کارکنان و مدیران شرکت‌ها و بازرسان قانونی که در انجام فعالیت خود به اسناد، مدارک و اطلاعات مشتری نزد شرکت‌ها دسترسی پیدا می‌کنند، موظفند با رعایت اصل امانت‌داری، رازداری و محرمانگی اسناد، مدارک و داده‌ها و اطلاعات مذکور و همچنین گزارش‌هایی را که بر اساس آنها تهیه می‌کنند به عنوان «اسرار حرفه‌ای» تلقی نمایند. افشای اسرار حرفه‌ای در صورت وجود الزام صریح قانونی و یا دستور مرجع قضایی امکان‌پذیر است.

ماده ۱۶- دریافت گزارش اعتباری مشتری توسط استفاده‌کنندگان و اشخاص ذی‌نفع، با رضایت مشتری یا نماینده قانونی ایشان امکان‌پذیر است. استفاده‌کنندگان و اشخاص ذی‌نفع موضوع این ماده موظفند با رعایت اصل امانت‌داری، رازداری و محرمانگی داده‌ها، اطلاعات اعتباری و گزارش اعتباری مشتری را محرمانه تلقی نموده و از افشای آن جز با رضایت مشتری یا نماینده قانونی ایشان خودداری نمایند. افشای اسرار محرمانه نزد مرجع یا مقام ذی‌صلاح در صورت وجود الزام صریح قانونی و یا دستور مرجع قضایی امکان‌پذیر است.

تبصره ۱- شرکت‌ها بدون اجازه مقام ناظر بر فرایند تأمین امنیت مجاز به ارائه و انتقال اسناد، مدارک و اطلاعات پشتوانه امتیاز اعتباری به استفاده‌کنندگان، تأمین‌کنندگان داده‌ها و اطلاعات و سایر اشخاص به استثنای شخص متقاضی یا نماینده قانونی وی نیستند.

تبصره ۲- هیچ یک از شرکت‌ها مجاز به نگاهداری و ذخیره‌سازی داده‌ها و اطلاعات موضوع پایگاه داده اعتباری نیستند. در غیر این صورت، مطابق با آیین‌نامه اعمال مقررات انتظامی متناسب با تخلفات شرکت‌های اعتبارسنجی و مدیران آنها موضوع تصویب‌نامه شماره ۱۹۲۴۴۷/ت/۶۵۲۳۴ هـ مورخ ۱۴۰۴/۱۱/۲۱ با آنان رفتار خواهد شد.

تبصره ۳- شرکت‌ها مکلفند روش‌های احراز هویت سامانه‌ای (سیستمی) را به همراه دلایل و مستندات کافی پس از تأییدیه مدیریت تطبیق و امنیت اطلاعات، به مقام ناظر بر فرایند تأمین امنیت جهت بررسی ارائه نمایند. مقام ناظر بر فرایند تأمین امنیت پس از بررسی درخواست ارائه‌شده، نتیجه درخواست را به همراه دلایل به شرکت‌ها اعلام می‌نماید. استفاده از روش احراز هویت پیشنهادی منوط به تأیید مقام ناظر بر فرایند تأمین امنیت خواهد بود.

تبصره ۴- شرکت‌ها موظفند پس از احراز هویت، امکان دریافت امتیاز اعتباری یا گزارش اعتباری مشتری را برای متقاضی و یا نماینده قانونی وی فراهم نمایند.

تبصره ۵- شرکت‌ها موظفند امکان دریافت امتیاز اعتباری یا گزارش اعتباری مشتری را برای استفاده‌کنندگان به صورت سامانه‌ای (سیستمی) به نحوی فراهم نمایند که پس از دریافت تأییدیه



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

۲۹۹۹۳

ت/۵۱۹۰هـ

شماره

تاریخ

۱۴۰۵ / ۳ / ۳۱

مشتری، گزارش اعتباری برای استفاده کنندگان قابل استفاده باشد. مدیران شرکتها و مدیر واحد تطبیق و امنیت اطلاعات مسئول نظارت بر حسن اجرای این ماده خواهند بود.

ماده ۱۷- اعطای دسترسی به استفاده کنندگان جهت استعلام امتیاز یا گزارش اعتباری مشتری منوط به عقد توافق نامه همکاری کتبی خواهد بود. مدیران شرکتها مسئول نظارت بر حسن اجرای این ماده در چارچوب قوانین و مقررات ذی ربط خواهند بود.

تبصره ۱- نمونه متن توافق نامه همکاری ظرف دو ماه پس از تاریخ ابلاغ این آیین نامه، توسط مقام ناظر بر فرایند تأمین امنیت تهیه و ابلاغ می گردد.

تبصره ۲- مقام ناظر بر فرایند تأمین امنیت مکلف است توافق نامه همکاری را به نحوی تدوین نماید که جزئیات تعهدات طرفین و الزامات حفاظت اطلاعات و حفظ محرمانگی و امنیت دادهها در آن قید شده باشد.

تبصره ۳- استفاده کنندگان مجاز به نگاهداری و ذخیره سازی گزارش اعتباری و امتیاز اعتباری نیستند و در صورت تخلف، شرکت مکلف است دسترسی آنها به خدمات را قطع نماید. این موضوع باید در متن توافق نامه همکاری نیز درج گردد.

ماده ۱۸- تغییرات مجاز در دادهها و اطلاعات شرکتها عبارت از به روز رسانی دادهها و اطلاعات از سوی تأمین کنندگان اطلاعات، اصلاحات موضوع ماده (۸) این آیین نامه، تصفیه دادهها و اطلاعات دریافتی از تأمین کنندگان دادهها و اطلاعات، امحاء گزارش اعتباری، امتیاز اعتباری و سایر محصولات تولید شده است. سایر مصادیق تغییرات مجاز دادهها و اطلاعات توسط مقام ناظر بر فرایند تأمین امنیت تعیین خواهد شد.

ماده ۱۹- شرکتها موظفند اسناد، دادهها و اطلاعات و مدارک پشتوانه امتیاز اعتباری را به سوابق الکترونیکی تبدیل نمایند و تا زمان تبدیل آن به سابقه الکترونیکی، اسناد، دادهها و اطلاعات و مدارک مذکور را با رعایت اصول امنیتی و حفاظت شده نگاهداری کنند.

ماده ۲۰- مدیریت تطبیق و امنیت اطلاعات موظف است ضوابط داخلی برای ذخیره، نگاهداری و حفاظت اسناد، دادهها و اطلاعات و مدارک را تدوین و به مدیران شرکتها جهت تصویب ارائه نماید.

ماده ۲۱- شرایط و ضوابط نگاهداری اسناد، دادهها و اطلاعات و مدارک در صورت وجود و سوابق الکترونیکی باید متناسب با شرایط استاندارد از قبیل قفسه بندی کافی، عاری از گرد و غبار و رطوبت، مجهز به سیستمهای اعلام و اطفای حریق و دارای سیستمهای حفاظتی و ایمنی مطابق با استانداردهای بین المللی مدیریت خطر (ریسک) فیزیکی مطلوب تنظیم گردد.

ماده ۲۲- مدیران شرکتها مکلفند ظرف زمان تعیین شده توسط مقام ناظر بر فرایند تأمین امنیت، نسبت به امحاء گزارش اعتباری، امتیاز اعتباری یا سایر محصولات تولید شده اقدام نمایند و



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره ۲۹۹۹۲
تاریخ ۱۳۰۵ / ۳ / ۳۱

در صورت تخلف، به یک یا چند مورد از اقدامات نظارتی موضوع جزء (۷-۵-۳) بند (ب) ماده (۲) قانون محکوم خواهند شد.

تبصره- مدیریت تطبیق و امنیت اطلاعات مکلف است گزارش اعتباری، امتیاز اعتباری یا سایر محصولات تولیدشده توسط شرکتها را به مدت پنج سال نگاهداری و پس از آن نسبت به انتقال آن به مقام ناظر بر فرایند تأمین امنیت اقدام نماید.

ماده ۲۳- شرکتها مکلف به امحاء اسناد، مدارک و دادهها و اطلاعات پشتوانه امتیاز اعتباری (اسناد و مدارک و یا سوابق الکترونیکی) ظرف یک هفته پس از اعلام رسمی شورا مبنی بر انحلال یا لغو مجوز فعالیت شرکت می باشد. شرکت موظف است ترتیبات امحای اسناد و مدارک و یا سوابق الکترونیکی را به نحوی اتخاذ نماید که امکان بازیابی مجدد آنها وجود نداشته باشد. مسئولیت تدوین و تصویب ضوابط مربوط به نحوه امحاء اسناد و مدارک و دادهها و اطلاعات پشتوانه امتیاز اعتباری بر عهده مدیران شرکتها بوده و مسئولیت حسن اجرای آن بر عهده مدیران قانونی وقت شرکت و با نظارت مقام ناظر بر فرایند تأمین امنیت است.

تبصره- شرکت موظف است در صورت درخواست مقام ناظر بر فرایند تأمین امنیت، تمام یا بخشی از اسناد، مدارک و دادهها و اطلاعات موضوع این ماده را به مقام ناظر بر فرایند تأمین امنیت به نحوی انتقال دهد که پس از انتقال، امکان دسترسی و استفاده از آنها توسط شرکت و سایر اشخاص وجود نداشته باشد.

ماده ۲۴- شرکتها مجاز به فروش گزارش اعتباری و یا تطبیق گزارش اعتباری با توجه به نیاز جامعه به استفاده کنندگان، صرفاً پس از انعقاد قرارداد رعایت اصول حفظ محرمانگی و حفاظت دادهها و اطلاعات که به تأیید مدیران شرکتها رسیده است، خواهند بود. همکاری با استفاده کنندگان و سایر شرکتها منوط به اجرای این قراردادها خواهد بود.

ماده ۲۵- انعقاد قرارداد مشاوره یا هر عنوان دیگر با پیمانکاران و مشاوران توسط شرکتها جهت توسعه و برآزش الگو (مدل) های محاسبه امتیاز اعتباری و نظایر آن، صرفاً در صورتی مجاز است که دادهها به صورت بدون نام (ناشناس) و بدون دسترسی از راه دور در اختیار مشاورین و پیمانکاران قرار گیرد. مدیران شرکتها مسئول نظارت بر حسن اجرای این ماده هستند.

تبصره- انعقاد قرارداد با مشاوران خارجی جهت توسعه و برآزش الگوی (مدل) محاسبه امتیاز اعتباری و نظایر آن، منوط به تأیید مقام ناظر بر فرایند تأمین امنیت خواهد بود. در صورت تأیید عقد قرارداد با مشاور خارجی، مدیریت تطبیق و امنیت اطلاعات موظف به نظارت مداوم بر رعایت الزامات امنیتی عملکرد مشاور خارجی خواهد بود. در هر صورت، دادهها باید ضمن رعایت فرایندهای این ماده، صرفاً به صورت بدون نام در اختیار مشاور خارجی قرار گیرد.

ماده ۲۶- انعقاد قرارداد مشاوره یا هر عنوان دیگر با پیمانکاران و مشاوران خارجی توسط شرکتها جهت توسعه، آزمون (تست) و بهروزرسانی نرم افزارها و سامانه های تخصصی مرتبط ممنوع است.



جمهوری اسلامی ایران

رئیس جمهور

تصویب نامه هیئت وزیران

شماره
تاریخ
۱۴۰۵ / ۳ / ۳۱

تبصره- توسعه و به روز رسانی نرم افزار و سامانه توسط مشاورین داخلی منوط به عدم خروج داده ها و اطلاعات از مرکز داده، اعم از رایانه های مرکزی (سرورهای) شرکت ها و عدم اعطای دسترسی از راه دور است. مدیریت تطبیق و امنیت اطلاعات مسئول نظارت بر حسن اجرای این ماده خواهد بود.

ماده ۲۷- هرگونه پشتیبانی و نگاهداری دائمی نرم افزارها و سامانه های تخصصی مرتبط شرکت ها از راه دور ممنوع است. دسترسی از راه دور به طور موقت به نرم افزارها و سامانه های مذکور در صورتی که مشاور یا پیمانکار تابعیت ایرانی داشته باشد، پس از تأیید مقام ناظر بر فرایند تأمین امنیت بلا مانع است. هرگونه دسترسی پیمانکاران در مرحله بهره برداری عملیاتی نرم افزارها و سامانه های تخصصی، بنا به ضرورت با نظارت و پایش (کنترل) کامل و با مسئولیت پذیری مدیران شرکت ها انجام می گردد.

ماده ۲۸- کلیه تجهیزات و زیرساخت های فناوری اطلاعات که توسط شرکت ها خریداری شده یا به هر نحوی مورد استفاده قرار می گیرد، قبل از بهره برداری توسط مدیریت تطبیق و امنیت اطلاعات مورد بررسی فنی قرار گرفته و در صورت تأیید، مورد استفاده قرار می گیرد.

ماده ۲۹- پیش از صدور مجوز فعالیت شرکت ها، دریافت داده ها و اطلاعات از تأمین کنندگان داده ها و اطلاعات، منوط به رعایت آیین نامه تأسیس و ارائه برنامه زمان بندی و اجرای این آیین نامه توسط مدیران شرکت ها خواهد بود. پس از صدور مجوز فعالیت شرکت های اعتبارسنجی، ظرف یک ماه برنامه اجرایی این آیین نامه توسط شرکت ها به مقام ناظر بر فرایند تأمین امنیت ارائه خواهد شد. در صورت امتناع یا عدم همکاری مدیران شرکت ها در اجرای مفاد این آیین نامه با مدیریت تطبیق و امنیت اطلاعات و مقام ناظر بر فرایند تأمین امنیت، پس از اعلام عدم همکاری توسط مقام ناظر بر فرایند تأمین امنیت به شورا، شورا یک یا چند مورد از اقدامات نظارتی موضوع جزء (۷-۵-۳) بند (ب) ماده (۲) قانون را در خصوص شرکت ها اتخاذ می نماید.

ماده ۳۰- مدیریت تطبیق و امنیت اطلاعات مکلف است هر سه ماه یکبار گزارش عملکرد شرکت ها را در زمینه امنیت اطلاعات مطابق با این آیین نامه، برای مقام ناظر بر فرایند تأمین امنیت ارسال نماید.

ماده ۳۱- شرکت ها موظفند با نظارت مدیریت تطبیق و امنیت اطلاعات و به منظور پیشگیری از آسیب های شغلی مدیران و کارکنان تحت امر، دوره های آموزشی متناسب را تدارک ببینند.

ماده ۳۲- شرکت ها موظف به رعایت مفاد آیین نامه طرز نگاهداری اسناد سری و محرمانه دولتی و طبقه بندی و نحوه مشخص نمودن نوع اسناد و اطلاعات مصوب ۱۳۵۴ با اصلاحات بعدی و مفاد آیین نامه اجرایی حفاظت اسناد و مدارک طبقه بندی شده مصوب شماره (۲۷۲) شورای عالی امنیت ملی با اصلاحات بعدی می باشند.