مقررات اجرایی تأمین ایمنی و سلامت ارسال پیامک انبوه درشبکه‌های ارتباطی

با استناد به مفاد سند «سیاست‌های ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه در شبکه‌های ارتباطی»، مصوبه مورخ ۱۳۹۳/۱۱/۱ شورای عالی فضای مجازی و با هدف ارتقای سلامت و ایمنی خدمات ارسال پیامک در شبکه‌های ارتباطی و نیز صیانت از حریم خصوصی کاربران و پیشگیری از وقوع جرم در بسترهای خدمات پیامکی، «مقررات اجرایی تأمین ایمنی و سلامت ارسال پیامک انبوه در شبکه‌های ارتباطی» به شرح این سند در جلسات ۲۳ الی ۲۸ در کارگروه موضوع ماده ۲ مصوبه مذکور، بررسی و به تصویب رسید.

ماده ۱) تعاریف

- **ارائه دهندگان خدمات ارتباطی:** دارندگان پروانه ایجاد و بهره برداری از شبکه‌های ثابت و همراه از وزارت ارتباطات و فناوری اطلاعات.
- **کارگروه:** کارگروه موصوف در بند ۲ سیاست‌های ساماندهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه‌های ارتباطی، مصوب ۱۳۹۳/۱۱/۱ شورای عالی فضای مجازی.
- **پیام‌رسان:** اشخاص موضوع جزء «ت» بند ۱ مصوبه جلسه بیست و یکم شورای عالی فضای مجازی که خدمات پیامکی انبوه و ارزش‌افزوده را از طریق شبکه ارائه‌کننده خدمات ارتباطی به پیام پرداز را ارائه می‌کنند.
- **پیام پرداز**: شخص حقیقی یا حقوقی که پیام را برای پیام‌رسان پدید می‌آورد و یا پردازش و یا گردآوری و به آن واگذار می کند. در جایی که پیام رسان راسا پیام پردازی می‌کند مشمول این عنوان خواهد بود.
- **احراز هویت:** فرآیندی که طی آن شناسایی و تطبیق مشخصات پیام‌پرداز در فرآیند پیام‌پردازی و پیام-رسانی، انجام می‌شود.
- **مقررات مدیریت امنیت پیام‌رسان‌ها:** به مجموعه الزامات و اقداماتی گفته می‌شود که می‌بایست توسط مدیریت پیام‌رسان در ساختار و شیوه‌های اجرایی پیاده‌سازی شوند.
- **مقررات فنی ـ امنیتی پیام‌رسان‌ها:** : به مجموعه الزامات و اقداماتی گفته می‌شود که با پیاده‌سازی آن‌ها سطح امنیت پیام‌رسان در ابعاد کاربری، نرم‌افزار، سخت‌افزار و زیرساخت افزایش پیدا خواهد کرد.
- **مقررات انتظامی پیام‌رسان‌ها:** به مجموعه الزامات و اقداماتی گفته می‌شود که پیاده‌سازی آن‌ها موجب انتظام‌بخشی و ساماندهی اجرایی در فرآیند فعالیت پیام‌رسان و پیام پردازان خواهد شد.

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک ۷۶، ساختمان شماره ۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

ماده ۲) احراز هویت

۱. ارائه دهنده خدمات ارتباطی مکلف است جهت ارائه شماره پیامکی، متقاضی پیام‌پردازی را بصورت حضوری احراز هویت نماید

تبصره۱: درصورتی که زیرساخت های لازم برای احراز هویت غیرحضوری فراهم شود الزامی به حضور نخواهد بود.

تبصره۲: احراز هویت اشخاص حقوقی، تنها با درخواست رسمی سازمان یا دستگاه مربوطه میسر خواهد بود.

۲. پیام‌رسان مکلف است صرفا به اشخاصی که تاییدیه احراز هویت حضوری از ارائه‌دهنده خدمات ارتباطی را اخذ نموده‌اند خدمت ارائه نماید

تبصره: پیام‌رسان مکلف است نسبت به احراز هویت خدمت‌گیرندگان(پیام‌پرداز) پیشینی خود ظرف مدت ۳ ماه از زمان ابلاغ این مصوبه اقدام نمایند.

۳. پیام‌رسان در هنگام واگذاری سرشماره می‌بایست هویت پیام‌پرداز را با ارسال پیامک به شماره تلفن همراه ایشان احراز نماید.

۴. پیام‌رسان موظف است برای شفافیت امور مالی، تطابق حساب بانکی به نام پیام‌پرداز را احراز هویت نماید.

۵. تمامی پیام‌رسان‌ها مکلف‌اند از واگذاری شماره به پیام‌پرداز متخلف که از سوی دبیرخانه کارگروه اعلام می‌گردد خودداری نماید.

۶. ارائه‌دهنده خدمات ارتباطی اطلاعات پیام‌پرداز را پس از واگذاری سرشماره می‌بایست بصورت آنی در سامانه وزارت فرهنگ و ارشاد اسلامی ثبت نماید.

۷. پیام‌رسان مکلف است هر شماره پیامکی را تنها به یک نفر شخص حقیقی یا حقوقی اختصاص دهد.

۸. تعداد کل خطوط قابل واگذاری به اشخاص حقیقی و حقوقی در تمامی پیام‌رسان‌ها به شرح ذیل می‌باشد:

الف: اشخاص حقیقی ۲ شماره.

ب: اشخاص حقوقی بخش خصوصی ۱۰ شماره.

پ: دستگاه‌های موضوع ماده ۲۹ قانون برنامه ۵ ساله ششم توسعه کشور بدون محدودیت می‌باشند.

تبصره : برای تعداد خطوط بیش از تعداد ذکر شده مجوز کارگروه الزامیست.

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک۷۶، ساختمان شماره۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

۹. ارسال پیام منتسب به سازمان‌های عمومی و دولتی تنها با استفاده از پروفایل احراز هویت شده حقوقی همان سازمان در پیام‌رسان انجام شود.

۱۰. ثبت‌نام و استفاده از خدمات پیام‌رسان تنها با I P ایران باشد و به‌هیچ‌وجه با I P غیر از ایران خدمات ارائه نشود.

۱۱. مجوز فعالیت پیام‌رسان، مالکیت نرم‌افزار کاربردی و درگاه پرداخت آن می‌بایست به نام پیام‌رسان یا نماینده قانونی آن باشد.

ماده ۳) صیانت محتوایی در پیامک‌های انبوه

۱. نظارت بر اساس کلیدواژهای حساس و غیرمجاز بر روی پیامک‌ها، قبل از ارسال توسط پیام‌رسان اعمال گردد.

تبصره: این کلیدواژه‌ها با نظر دستگاه‌های عضو و از طریق سامانه کارگروه به پیام‌رسان‌ها اعلام می‌شود.

۲. پیامک‌های حاوی لینک با هدف جلوگیری از اعمال مجرمانه قبل از انتشار توسط پیام‌رسان مورد بازبینی قرار گیرد. همچنین لینک‌های مجاز در محتوای پیامک می‌بایست ازلحاظ آلوده بودن به ویروس، بدافزار و فیشینگ امن باشد.

۳. ارسال هرگونه پیامک حاوی محتوای مجرمانه مطابق فهرست مصادیق محتوای مجرمانه مصوب کارگروه تعیین مصادیق و مصوبات این کارگروه، ممنوع بوده و پیام‌رسان مکلف است با اتخاذ تدابیر مناسب از ارسال این گونه پیامک‌ها جلوگیری نماید.

۴. در صورت ارسال پیامک با محتوای مجرمانه توسط پیام‌پرداز حقیقی یا حقوقی، پیام‌رسان موظف است از طریق سرشماره آن پیام‌رسان، بلافاصله به‌تمامی دریافت‌کنندگان پیامک مذکور، یک پیامک جبرانی با محتوای اطلاع‌رسانی در خصوص مجرمانه بودن پیامک قبلی و راهکار مقابله با آن ارسال نماید.

تبصره : در صورت ارسال هرگونه پیامک مجرمانه از سوی پیام‌پرداز، پیام‌رسان مکلف است بلافاصله سرشماره، متن و تعداد پیامک ارسال‌شده را از طریق پنجره واحد به پلیس فتا اعلام کند (تا قبل از راه‌اندازی سامانه برخط این کار از مسیر اعلامی پلیس فتا انجام می‌شود)

۵. پیام‌رسان مکلف است ضمن ایجاد دسترسی برخط برای نظارت، یک رونوشت از پیامک انبوه را نیز، بصورت برخط به سامانه وزارت فرهنگ و ارشاد اسلامی ارسال نماید.

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک ۷۶، ساختمان شماره ۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

ماده۴) مدیریت امنیت ارسال پیامک انبوه

پیام رسان مکلف است در راستای اهداف تعیین شده، نسبت به تأمین مدیریت امنیت با لحاظ شاخص‌های زیر اقدام نماید:

ردیف	عنوان شاخص	شرح شاخص
۱	ایجاد جایگاه سازمانی امنیت اطلاعات	ایجاد جایگاه سازمانی مناسب برای امنیت اطلاعات، زیر نظر مدیرعامل و تعیین فردی به‌عنوان مسئول امنیت[۱]
۲	دریافت گواهینامه امنیتی و ممیزی	دریافت گواهی استاندارد مورد تأیید مرکز افتا. (مانند گواهی استاندارد ISMS I SO ۲۷۰۰۱)
۳	تدوین و تعهد به خط‌مشی امنیت اطلاعات	تدوین خط‌مشی امنیت اطلاعات شرکت(پیام‌رسان) و تعهد مدیریت به ارتقاء مداوم امنیت اطلاعات، و تصویب آن توسط بالاترین مقام مسئول شرکت. این خط مشی می‌بایست حداقل شامل موارد زیر باشد: ۳.۱)هرگونه تغییر و یا توسعه در سامانه‌ها و زیرساخت‌های موجود باید توسط مسئول امنیت اطلاعات به‌صورت مستند مورد تأیید امنیتی قرار گیرد. ۳.۲) ارائه و یا دریافت خدمات به طرف‌های ثالث و واگذاری حقوق دسترسی به آن‌ها باید بر مبنای یک سازوکار مشخص شامل قرارداد منع افشا، قرارداد حفظ محرمانگی و ... باشد و ضمن حفظ حریم خصوصی و رعایت اصل حداقل دسترسی به‌صورت مستند به تأیید مسئول امنیت اطلاعات برسد. ۳.۳)در صورت خاتمه همکاری/قرارداد/توافق‌نامه هر یک از کارکنان، پیمانکاران و طرف‌های ثالث باید تمامی دسترسی آن‌ها به صورتی که لاگ فعالیت‌های قبلی آنان از بین نرود، قطع شود. ۳.۴)به‌محض تغییر شغل و یا ماهیت کاری، دسترسی‌ها می‌بایست بر اساس اصل حداقل دسترسی مجدداً تنظیم و تعریف شود.
۴	تعهد کارکنان به حفظ محرمانگی	رعایت موارد زیر برای استخدام کارکنان، توسط پیام‌رسان: ۴.۱)ارائه عدم سوءپیشینه از مراجع ذی‌صلاح برای کارکنان بخش امنیت ۴.۲)توجیه و تنظیم تعهدنامه منع افشا و حفظ محرمانگی توسط تمامی افراد فعال در شرکت نسبت به مسائل امنیت اطلاعات
۵	آمادگیِ واکنش به حوادث بحرانی	تهیه، به روزرسانی و در معرض قرار دادن موارد زیر: ۵.۱)فرآیندهای مقابله با حوادث بحرانی

[۱] بر اساس ماده ۱۴۳ قانون مجازات اسلامی«در مسئولیت کیفری اصل بر مسئولیت شخص حقیقی است و شخص حقوقی در صورتی دارای مسئولیت کیفری است که نماینده قانونی شخص حقوقی به نام یا در راستای منافع آن مرتکب جرمی‌شود. مسئولیت کیفری اشخاص حقوقی مانع مسئولیت اشخاص حقیقی مرتکب جرم نیست.» (مسئولیت کیفری اشخاص حقوقی مانع مسئولیت اشخاص حقیقی مرتکب جرم نیست)

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس:۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک۷۶، ساختمان شماره۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

ردیف	عنوان شاخص	شرح شاخص
		۵.۲)فهرست افراد کلیدی و شماره تماس‌های آن‌ها و همچنین شماره‌های امدادی
۶	آموزش و توانمندسازی	طراحی و اجرای برنامه‌های آموزش و توانمندسازی در موارد زیر: ۶.۱)آموزش کارکنان پیام‌رسان در خصوص حملات مبتنی بر روش‌های مهندسی اجتماعی و سایر موضوعات موردنیاز برای ارتقای امنیت و سلامت فعالیت پیام‌رسان ۶.۲)آموزش پیام‌پردازان در خصوص استفاده ایمن از پیام‌رسان و مخاطرات آن

ماده۵) الزامات فنی ـ امنیتی ارسال پیامک انبوه

پیام رسان مکلف است در راستای اهداف تعیین شده، نسبت به تأمین شاخص‌های فنی حصول امنیت ارسال پیامک به شرح زیر اقدام نماید:

ردیف	عنوان شاخص	شرح شاخص
۱.	تهیه و به روزرسانی مستمر نقشه منطقی و فیزیکی شبکه	تهیه و به‌روزرسانی مستمر نقشه‌های منطقی و فیزیکی شبکه، سامانه‌ها، وب‌سرویس‌ها، برنامه‌های کاربردی و مسیرهای اتصال به دیگر شبکه‌ها و فهرستی از تمامی اجزای شبکه (شامل تجهیزات، سرورها و ...).
۲.	استفاده از سرویس میزبانی حداقلی	میزبانی تمامی سرویس‌ها و سامانه‌ها در داخل کشور انجام شود. عدم رعایت این بند می‌بایست با دلیل موجه و قابل دفاع و مورد تأیید پلیس فتا باشد.
۳.	مدیریت دسترسی ایمن و حداقلی	بر اساس ماهیت کاری و سطوح امنیت اطلاعات در پیام‌رسان، حیطه‌بندی در دسترسی‌های موردنیاز به شرح زیر تعریف و رعایت شود: ۳.۱)کنترل تردد نقاط ورودی و خروجی و محل نگهداری اسناد و تجهیزات شبکه‌ای و سروری، با استفاده از شیوه‌های مختلف ازجمله دوربین مداربسته با قابلیت ذخیره‌سازی مناسب. ۳.۲)کنترل دسترسی در سطح شبکه به برنامه‌های کاربردی و پایگاه داده و نیز دسترسی از راه دور به سامانه‌ها. ۳.۳)دسترسی فیزیکی کنترل‌شده به تجهیزات شبکه و سرورها. ۳.۴)دسترسی مدیریتی از راه دور به درگاه‌های پیکربندی تجهیزات، سرویس‌ها و سیستم‌عامل‌ها براساس احراز هویت دوعاملی و اصل دسترسی حداقلی.
۴.	کنترل محیط‌های توسعه، تست و عملیات	• جداسازی محیط‌های توسعه، تست و عملیات به‌صورت فیزیکی و منطقی • تغییر شناسه‌های کاربری و کلمات عبور مورد استفاده در محیط تست و توسعه همزمان با انتقال به محیط عملیاتی و کاربردی. • عدم به‌کارگیری داده‌های محرمانه در محیط‌های تست و توسعه.
۵.	امن سازی تجهیزات	امن سازی تمامی تجهیزات شبکه و امنیت شبکه، سامانه‌ها و برنامه‌های کاربردی بر اساس استانداردهای امنیتی و بروزرسانی مستمر آن.

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک۷۶، ساختمان شماره۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

ردیف	عنوان شاخص	شرح شاخص
۶.	ارزیابی امنیتی	دریافت تأییدیه ارزیابی امنیتی کلیه تجهیزات شبکه‌ای، سامانه‌ای، وب‌سرویس‌ها و برنامه‌های کاربردی به‌صورت سالیانه از آزمایشگاه‌های مورد تأیید پلیس فتا.
۷.	پشتیبان گیری	پشتیبان‌گیریِ منظمِ حداقل هفتگی بر اساس استانداردهای امنیتی و خط‌مشی امنیتی شرکت از پایگاه داده‌ها، لاگ‌ها و پیکربندی تجهیزات شبکه‌ای و نگهداری امن آنها تا شش ماه.
۸.	انقضای نشست	تدوین و اجرای سیاست و الگوی مدیریت نشست‌های پیام‌پردازان در سامانه‌های پیام‌رسان‌ها، مطابق با استانداردها و روش‌های امنیتی متناسب.
۹.	آنتی‌ویروس	نصب و به‌روزرسانی مداوم آنتی‌ویروس معتبر بر روی تمامی سیستم‌عامل‌ها و نرم‌افزارهای کاربردی.
۱۰.	به‌روزرسانی	به‌روزرسانی مستمر در تمامی سیستم‌عامل‌ها و مؤلفه‌های نصب‌شده بر روی آن‌ها، تجهیزات و سامانه‌های سطح شبکه، مطابق با اصول مدیریت وصله.
۱۱.	شبکه بی‌سیم	تمهید و اجرای الزامات امن سازی شبکه بی‌سیم، در صورت استفاده از این ابزارها.
۱۲.	امنیت کلمه عبور پایگاه داده و پیام‌پردازان	• پرهیز از استفاده از کلمات عبور واضح و ساده در پایگاه داده‌ها. • تغییر نام کاربری و کلمه عبور پیش‌فرض بلافاصله بعد از نصب پایگاه داده. • اجرای فرآیند بازیابی رمز عبور بر اساس استانداردها و با استفاده از روش‌های امن.
۱۳.	امحاء	ایجاد فرایندی امن و مستند برای امحاء تجهیزات ذخیره‌سازی و مستنداتی که حاوی اطلاعات خصوصی پیام‌پردازان و یا سایر اطلاعات حساس پیام‌رسان می‌باشند.
۱۴.	استناد پذیری ادله دیجیتال	ثبت و نگهداری دسترسی‌های افراد به سیستم‌ها و داده‌ها، در سطح سیستم‌عامل‌ها، پایگاه‌های داده، وب سرورها، برنامه‌های کاربردی و تجهیزات شبکه‌ای و امنیتی و رعایت مواد ۶۶۷ و ۶۶۸ قانون آئین دادرسی کیفری(بخش آئین دادرسی جرائم رایانه‌ای).
۱۵.	همسان‌سازی ساعت	تنظیم تاریخ و زمان تمامی سرورها، تجهیزات شبکه‌ای و امنیتی، سامانه‌ها و برنامه‌های کاربردی، مطابق یک سیستم هم‌زمان‌سازی یکسان.
۱۶.	گواهینامه امنیتی محصول	• اخذ گواهینامه ارزیابی امنیتی برای پلتفرم مورداستفاده توسط پیام‌رسان • تهیه و نگهداری گزارش تست نفوذ بر روی شبکه و سامانه و اجرای عملیات مدیریت وصله‌ها به‌صورت نوبه‌ای برای ارائه به مراجع ذی‌صلاح حسب نیاز (در صورت تغییر در هریک در مرور زمان، تست نفوذ مجدداً اجرا و گزارش ارائه خواهد شد)

ماده ۶) الزامات انتظامی ارسال پیامک انبوه

ردیف	عنوان الزام	توضیحات
۱.	رمز یک‌بارمصرف	• پیام‌رسان مکلف است قبل از ارسال پیامک انبوه هویت پیام پرداز را با ارسال پیامک به شماره تلفن تأییدشده ایشان با سامانه شاهکار، احراز نماید.

ردیف	عنوان الزام	توضیحات
		• ورود به‌حساب کاربری پیام پرداز به‌صورت دومرحله‌ای، با استفاده از رمز یک‌بارمصرف پیامکی به شماره تلفن تأییدشده ایشان انجام شود. • از کپچا در تمامی فرم‌های ورود اطلاعات ازجمله صفحه ورود به‌حساب کاربری استفاده شود.
۲.	اعتبارسنجی	پیام‌رسان باید همه پیام‌پردازان را بر اساس ضوابطی که به تصویب کارگروه می‌رسد، اعتبارسنجی نموده و حدود سقف مجاز ارسال پیامک روزانه را برای آن‌ها اعمال کند.
۳.	استعلام برخط سیستمی	پیام‌رسان مکلف است پاسخ‌گویی به استعلامات قضایی را از طریق سامانه معرفی شده از طرف دبیرخانه کارگروه ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه فراهم کند.
۴.	صیانت از داده‌های پیام پرداز	• سیاست‌های لازم جهت حفظ حریم خصوصی پیام‌پردازان و جلوگیری از نشت اطلاعات برابر قوانین و مقررات جاری کشور و الزامات انتظامی پلیس فتا اتخاذ شود. • سوءاستفاده تجاری (فروش، معاوضه، اجاره و ...) از اطلاعات خصوصی پیام‌پردازان تحت هر عنوان و شکل ممکن ممنوع است. • چگونگی اخذ، دسترسی و بهره‌برداری پیام‌پرداز و پیام‌رسان از فهرست مخاطبین، براساس مصوبه کارگروه با عنوان «ضوابط دسترسی به فهرست مخاطبین» می باشد.
۵.	به اشتراک‌گذاری تجربیات	پیام‌رسان و پیام‌پردازان شگردهای مجرمانه و تخلفات شناسایی شده و تجربیاتی که می‌تواند به امنیت پیام‌رسانی در شبکه‌های ارتباطی کمک نماید را به گونه‌ای که دبیرخانه کارگروه تعیین می‌کند، با دیگر پیام‌رسان‌ها و پیام‌پردازان و پلیس فتا به اشتراک بگذارند.
۶.	شکایات مردمی	سازوکار لازم جهت ایجاد بستر ارتباط با مشتری و رسیدگی به شکایات پیام‌پردازان تعریف و پیاده‌سازی شود.
۷.	واکنش به حملات سایبری	به‌محض اطلاع از وجود شواهد نفوذ، درز اطلاعات و یا هرگونه حادثه سایبری دیگر، موضوع به مرکز فوریت‌های سایبری پلیس فتا (شماره تماس ۰۹۶۳۸۰ و یا سامانه https://csirc.cyberpolice.ir) اعلام و انتشار هرگونه اخبار در این خصوص با هماهنگی و مشورت کارشناسان پلیس فتا صورت گیرد.
۸.	ورود و خروج	ورود و خروج افراد و کارکنان، به محل شرکت ثبت و نگهداری شود.
۹.	بستر پرداخت مالی	پیام‌رسان باید بستر پرداخت مالی امن برای استفاده پیام‌پردازان ایجاد نماید.

ماده ۷) نگاشت نهادی برای تحقق مقررات اجرایی

دبیرخانه کارگروه

۱. ایجاد پنجره واحد نظارت بر پیام‌رسانی در شبکه‌های ارتباطی با امکان اعلام مصادیق مجرمانه و تخلفات احتمالی به پیام‌رسان و کنترل دامنه جرائم مرتبط
۲. نظارت محتوایی پیامک باهدف ارتقای امنیت و سلامت پیام‌رسانی در شبکه‌های ارتباطی
۳. معرفی پیام‌رسان‌های مورد تأیید به پلیس فتا جهت طی فرآیند ارزیابی فنی ـ امنیتی

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک۷۶، ساختمان شماره۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵

پلیس فضای تولید و تبادل اطلاعات ناجا

۱. ممیزی و نظارت بر رعایت الزامات امنیت فنی ارسال پیامک انبوه مندرج در این سند
۲. صدور گواهینامه امنیت پیام‌رسان به‌صورت سالیانه مبنی بر رعایت الزامات مذکور در سند حاضر توسط پیام‌رسان
۳. جلب همکاری پیام‌رسان‌ها برای کنترل دامنه جرائم محتوایی پیامکی
۴. اعلام هشدارهای امنیتی به پیام‌رسان‌ها و پیگیری رفع آن‌ها
۵. معرفی مراجع مورد تأیید جهت ارزیابی الزامات اجرایی ماده ۵ این سند
۶. پیشنهاد بازنگری الزامات امنیت فنی ارسال پیامک به کارگروه به صورت سالیانه در صورت نیاز
۷. گزارش به کارگروه «ساماندهی خدمات پیامکی ارزش‌افزوده و پیامک انبوه در شبکه‌های ارتباطی» هر شش ماه یک‌بار
۸. فراهم نمودن امکان آموزش به کارشناسان پیام‌رسان‌ها

سایر دستگاه‌های عضو کارگروه

۱. همکاری با دبیرخانه در اجرای این مقررات
۲. ارائه پیشنهاد برای اصلاح و تکمیل این مقررات
۳. بررسی و صیانت محتوایی در راستای ماموریت‌های ذاتی
۴. وزارت ارتباطات و فناوری اطلاعات مکلف است سازوکار ایجاد ارتباط با سامانه شاهکار جهت اخذ استعلام تعداد خطوط هر شخص را در اختیار پیام‌رسان قراردهد.

پیام‌رسان

۱. دریافت گواهینامه امنیت فنی از پلیس فتا به‌صورت سالیانه
۲. پیاده‌سازی الزامات مندرج در این مصوبه حداکثر سه ماه پس از ابلاغ آن
۳. استمرار و به روز نگه‌داری اجرای الزامات این سند در تمامی سکوهای ارائه‌شده به پیام پرداز از قبیل وب‌سایت، وب‌سرویس، برنامه‌های موبایلی، افزونه، نرم‌افزار و ...

۱) تهران، میدان بهارستان، خیابان کمال الملک، ساختمان وزارت فرهنگ و ارشاد اسلامی، طبقه دوم، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۳۳۹۶۶۰۶۸ تلفکس: ۳۳۹۶۶۲۴۶
۲) تهران، خیابان سمیه، روبروی برج سپهر، پلاک ۷۶، ساختمان شماره ۲، مرکز توسعه فرهنگ و هنر در فضای مجازی تلفن: ۴۵۲۶۸ ۸۸۳۱۵۹۳۱-۴ تلفکس: ۸۸۳۱۵۹۳۵