چهارشنبه پانزدهم مرداد ماه ۱۳۹۳

سال هفتادم شماره ۲۰۲۱۸

(۷۰۳)

قوّهٔ قضائیه

روزنامهٔ رسمی جمهوری اسلامی ایران

شامل: قوانین ـ مذاکرات مجلس شورای اسلامی ـ رویه‌های قضائی ـ عهدنامه‌ها ـ آئین‌نامه‌ها

تصویب‌نامه‌ها ـ تصمیم‌نامه‌ها ـ اساسنامه‌ها و آگهیها

WWW.RRK.IR
WWW.DASTOUR.IR

تک شماره ۱۰۰ تومان

قوانین و مقررات عمومی

شماره ۹۰۰۰/۳۸۴۶۳/۱۰۰ ۱۳۹۳/۵/۱۳

جناب آقای سینجلی جاسبی

رئیس محترم هیأت مدیره و مدیرعامل روزنامه رسمی کشور

تصویر آیین‌نامه شماره ۹۰۰۰/۲۸۱۹۹/۱۰۰ـ ۱۳۹۳/۵/۱۲ ریاست محترم قوه قضائیه جهت درج در روزنامه رسمی به پیوست ارسال می‌گردد.

مدیرکل دبیرخانه قوه قضائیه ـ محسن محدث

شماره ۹۰۰۰/۲۸۱۹۹/۱۰۰ ۱۳۹۳/۵/۱۲

آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی

در اجرای ماده ۵۴ قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی و بنا به پیشنهاد وزیر دادگستری، آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی به شرح مواد آتی است:

فصل اول: تعاریف

ماده۱ـ واژه‌ها و اصطلاحات بکار برده شده در این آیین‌نامه در معانی زیر بکار می‌رود:

الف ـ ارائه‌دهندگان خدمات دسترسی: اشخاصی هستند که امکان ارتباط کاربران را با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین‌المللی یا هر شبکه مستقل دیگر فراهم می‌آورند از قبیل تأمین‌کنندگان، توزیع‌کنندگان، عرضه‌کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.

ب ـ ارائه‌دهندگان خدمات‌میزبانی: اشخاصی هستند که امکان‌دسترسی کاربران به فضای ایجادشده توسط سامانه‌های‌رایانه‌ای، مخابراتی و ارتباطی تحت‌تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا رأساً یا توسط کاربر متقاضی، داده‌های رایانه‌ای را؛ جهت نگهداری، انتشار، توزیع یا ارائه در شبکه‌های داخلی یا بین‌المللی یا هر منظور دیگر ذخیره یا پردازش کنند.

ج ـ ارائه داده‌های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از داده‌های حفظ یا نگهداری‌شده توسط ارائه‌دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده‌ها را تحت تصرف یا کنترل دارند.

د ـ جمع‌آوری ادله الکترونیکی: فرآیندی است که طی آن ادله الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند.

هـ ـ زنجیره حفاظتی: مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذیصلاح به منظور حفظ صحت، تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی با بکارگیری ابزارها و روشهای استاندارد در مراحل شناسایی، کشف، جمع‌آوری، مستندسازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجراء درآورده و ثبت می‌کنند؛ به نحوی که امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد.

و ـ شنود: عبارت است از هر گونه دستیابی به محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا استفاده از سامانه‌ها و تجهیزات سخت‌افزاری و نرم‌افزاری مربوط.

ز- مجری حفاظت: شخصی است که به نحوی داده‌های رایانه‌ای ذخیره شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می‌شود.

ح - متصرف قانونی: در مورد اشخاص حقیقی، شخص مالک یا شخصی است که به نحوی داده یا سامانه را به صورت مشروع در اختیار دارد یا نماینده یا ولی یا سرپرست قانونی وی. در مورد اشخاص حقوقی دولتی یا عمومی غیردولتی، بالاترین مقام آنها یا نماینده قانونی آنها طبق مقررات مربوط و در مورد سایر اشخاص حقوقی، مدیر یا نماینده قانونی آنهاست.

ط - قانون: منظور از قانون در این آیین‌نامه، قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ می‌باشد.

تبصره - سایر اصطلاحات به شرح تعریف ارائه شده در قوانین دیگر می‌باشد.

فصل دوم: جمع‌آوری ادله الکترونیکی

الف: نگهداری داده‌ها

ماده۲- ارائه‌دهندگان خدمات دسترسی و میزبانی موظفند از سامانه‌هایی استفاده نمایند که قابلیت نگهداری داده‌های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد.

ماده۳- ارائه‌دهندگان خدمات دسترسی موظفند سامانه‌های خود را به نحوی تنظیم کنند که کلیه ارتباطات رایانه‌ای را که از طریق آنها انجام می‌شود ثبت کنند و کلیه داده‌های ترافیک مربوط به خود و کاربران مربوط را تا شش ماه پس از ایجاد نگهداری کنند.

تبصره - عرضه کنندگان خدمات دسترسی حضوری اینترنت (کافی‌نت‌ها) موظفند مشخصات هویتی، آدرس، ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی (IP) تخصیصی را در دفتر روزانه ثبت نمایند.

ماده۴- ارائه‌دهندگان خدمت دسترسی موظفند اطلاعات کاربران را حداقل ۶ ماه پس از خاتمه اشتراک یا لغو قرارداد کاربر نگهداری کنند. هویت و نشانی کاربر باید در قرارداد منعقده درج شود.

ماده۵ - ارائه دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه‌دهندگان خدمات میزبانی خارجی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند. برگه اشتراک باید به نحوی تنظیم شود که هویت و نشانی آنان مشخص باشد.

تبصره۱- ارائه‌دهندگان خدمات میزبانی موظفند سامانه‌های رایانه‌ای خود را به نحوی تنظیم کنند که هرگونه تغییر اعم از اصلاح یا حذف محتوا و داده ترافیک حاصل از آن را ذخیره نماید.

تبصره۲- اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می‌کنند، ارائه‌دهنده خدمات میزبانی محسوب نمی‌شوند.

ماده۶ - ارائه‌دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظفند امنیت داده‌های ترافیکی و محتوای نگهداری و حفاظت شده را مطابق با ضوابط و دستورالعمل‌هایی که به تصویب رئیس قوه قضائیه می‌رسد، تأمین نمایند.

ماده۷- داده‌های محتوا و ترافیک و اطلاعات کاربران باید مطابق مقررات این آیین‌نامه به نحوی نگهداری، حفاظت، توقیف و ارائه شود که صحت و تمامیت، محرمانگی، اعتبار و انکارناپذیری آنها محفوظ بماند.

ماده۸ - در مواردی که برابر قانون نگهداری و حفاظت داده‌ها الزامی است، نگهداری و حفاظت باید به گونه‌ای انجام شود که مدیریت جستجو و گزارش‌دهی آنها امکان‌پذیر باشد.

ماده۹- وزارت ارتباطات و فن‌آوری اطلاعات هماهنگی‌های لازم برای تنظیم زمان سامانه‌های جمع‌آوری داده‌های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می‌آورد.

ماده۱۰- مرکز آمار و فناوری اطلاعات با همکاری وزارت ارتباطات و فناوری اطلاعات سالانه رویه‌های فنی نحوه نگهداری، حفاظت، توقیف و ارائه داده‌ها و اطلاعات کاربران و همچنین راهنماهای عملی حفظ امنیت و استنادپذیری داده‌ها را تصویب و به ارائه‌دهندگان خدمات دسترسی و میزبانی و بهره‌برداران ابلاغ می‌نماید.

ب: حفاظت از ادله رایانه‌ای

ماده۱۱- مقام قضایی در جریان تحقیق و فرآیند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره شده را از جمله داده‌های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده‌هایی که نوع و نام آنها موقتاً تغییر یافته و یا داده‌هایی که برای بررسی آنها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید.

تبصره۱- ضابطان قضایی فقط در موارد مندرج در ماده ۳۴ قانون می‌توانند رأساً دستور حفاظت داده‌های ذخیره شده را صادر کنند.

تبصره۲- قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد.

ماده۱۲- دستور حفاظت باید به طور صریح و دقیق مشتمل بر نوع داده‌ها، موضوع و مدت زمان با رعایت تبصره۲ ماده ۳۴ قانون، باشد.

ماده۱۳- در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می‌شود.

ماده۱۴- مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجراء و صورت‌جلسه‌ای را مشتمل بر زمان اجرای دستور، نحوه حفاظت، حجم و نوع داده‌های حفاظت‌شده در دو نسخه تنظیم و یک نسخه از آن را به مرجع صادرکننده دستور ارسال کند و نسخه دیگر را نزد خود نگه دارد.

ماده۱۵- دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذینفع نیز ابلاغ می‌شود؛ مگر آن که ابلاغ به آنها مخل رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می‌باشد.

تبصره - روش مطمئن روشی است که با توجه به نوع داده‌ها و طول مدت زمان حفاظت، امکان بهره‌برداری از داده‌های حفاظت شده را در مراحل بعدی دادرسی ممکن سازد.

ماده۱۶- حفاظت از داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود.

ج: ارائه ادله رایانه‌ای

ماده۱۷- دستور ارائه توسط مقام قضایی صادر می‌شود و باید به طور صریح و شفاف و مشتمل بر شخص ارائه‌دهنده، موضوع و نوع داده‌ها، شیوه و زمان تحویل داده‌ها و مرجع تحویل گیرنده باشد.

ماده۱۸- ارائه داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شده و حتی‌الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه به یکی از شیوه‌های ذیل باشد:

الف - تحویل یک نسخه چاپ شده از داده.

ب - تحویل یک نسخه رایانه‌ای از داده.

ج - ایجاد دسترسی به داده.

د - انتقال تجهیزات رایانه‌ای و مخابراتی.

ماده۱۹- هنگام ارائه داده‌ها صورت‌جلسه‌ای در سه نسخهٔ تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه دهنده و تحویل گیرنده می‌رسد:

الف - شماره و تاریخ دستور قضایی ارائه داده‌ها

ب - مشخصات ارائه دهنده

ج - مشخصات تحویل گیرنده

د - زمان و مکان ارائه

هـ - نوع و حجم داده‌ها

و- اطلاعات مربوط به نحوه حفظ یا نگهداری داده‌ها

ز - روشهای امنیتی بکاررفته در زمان ارائه

ح - مشخصات سخت‌افزاری و نرم‌افزاری تجهیزات

ط - شیوه ارائه و مشخصات داده.

تبصره۱- در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها بعمل می‌آید.

تبصره۲- یک نسخه از صورت‌جلسه به مرجع قضایی ارسال می‌شود و نسخه‌ای در اختیار ارائه دهنده و نسخه دیگر در اختیار تحویل گیرنده قرار می‌گیرد.

ماده۲۰- از زمان ارائه داده‌ها به ضابطان قضایی یا دیگر اشخاص ذیربط، مسئولیت حفظ داده‌های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود.

ماده۲۱- ارائه داده‌هایی که افشاء یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توأم با تشریفات می‌باشد، تابع مقررات مربوط است.

ماده۲۲- دستور ارائه داده، مجوز افشای آن نمی‌باشد و پس از دستور ارائه هرگونه دسترسی به مفاد داده مستلزم صدور دستور قضایی است.

ماده۲۳- اشخاصی که مسئول اجرای هریک از دستورات قضایی اعم از نگهداری، حفاظت، ارائه، تفتیش و توقیف سامانه و داده یا شنود آن می‌باشند یا دستور به آنها ابلاغ می‌شود یا به نوعی مرتبط با دستورات یاد شده هستند، حق افشای مفاد دستور و یا داده‌ها و اطلاعات مربوط را ندارند.

د: تفتیش و توقیف ادله رایانه‌ای

ماده۲۴- ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاب می‌نماید در درخواست خود اعلام نمایند. همچنین، موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند:

الف - دلایل ضرورت تفتیش و توقیف

ب ـ حتی‌الامکان نوع و میزان داده‌ها و سخت‌افزارها
ج ـ محل تفتیش یا توقیف
د ـ دلایل لازم برای تصویربرداری و بررسی در خارج از محل
هـ ـ زمان تقریبی لازم برای تفتیش و توقیف.

ماده۲۵ـ در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی‌الامکان در محل استقرار سامانه انجام پذیرد.

ماده۲۶ـ مدت توقیف و فرصت اجرای تفتیش باید در دستور قضایی تصریح و کمترین فرصت ممکن منظور شود. در صورت نیاز به زمان بیشتر، به درخواست مجری تفتیش یا توقیف و ذکر علت آن، این مدت قابل تمدید می‌باشد.

ماده۲۷ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

ماده۲۸ـ در مواردی که تفتیش یا توقیف طبق دستور قضایی بدون حضور متصرف قانونی یا شخصی که داده یا سامانه را تحت اختیار دارد، انجام پذیرد، مراتب پس از انجام فوراً به ذینفع ابلاغ خواهد شد.

ماده۲۹ـ چنانچه پس از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی بیم لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی برود مراتب از مرجع قضایی صادرکننده دستور توقیف کسب تکلیف شده و در صورت تشخیص قاضی حسب مفاد ماده ۴۴ قانون عمل می‌گردد.

ماده۳۰ـ قوه قضاییه تمهیدات لازم از جمله بسترسازی و ایجاد زیرساختهای ارتباط رایانه‌ای و الکترونیکی و همچنین راه‌اندازی سامانه‌ها و درگاههای مبتنی بر فناوری اطلاعات را جهت تسهیل در عملیاتی کردن فرایندها و روشهای موضوع این آیین‌نامه فراهم می‌آورد.

ماده۳۱ـ اشخاصی که داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می‌باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان‌پذیر نباشد، نحوه دسترسی به داده‌ها یا سامانه‌ها از قبیل ورود به محل، رفع موانع استفاده از سخت‌افزار و نرم‌افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد.

ماده۳۲ـ رعایت متصرف قانونی سامانه موضوع بند ج ماده ۴۱ قانون، باید کتبی و با امضای وی باشد.

ماده۳۳ـ در مواردی که توقیف داده‌ها به روش چاپ یا کپی یا تصویربرداری داده‌ها انجام می‌شود، اصل داده‌ها در صورتی توقیف و غیرقابل دسترس می‌شود که در دستور قضایی تصریح شده باشد.

ماده۳۴ـ ضابطان صرفاً مجاز به تفتیش و توقیف داده‌ها و سامانه‌هایی هستند که به طور صریح در دستور قضایی ذکر گردیده و چنانچه حین اجرای دستور، داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی تحت کنترل یا تصرف متهم کشف شود، در صورت بیم امحاء نسبت به حفظ فوری داده‌ها اقدام و مراتب را حداکثر ظرف ۲۴ ساعت کتباً به مقام قضایی مربوط گزارش می‌دهند.

ماده۳۵ـ تفتیش داده‌ها یا سامانه‌ها در محل استقرار یا از طریق شبکه یا در آزمایشگاه یا در محل مناسب با دستور و تشخیص مقام قضایی با رعایت صحت، تمامیت، محرمانگی، انکارناپذیری ادله انجام می‌پذیرد.

ماده۳۶ـ ضابطان و اشخاصی که حسب قانون مأمور جمع‌آوری، تفتیش، نگهداری، حفظ و انتقال داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی می‌شوند باید علاوه بر داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم را در اختیار داشته باشند.

ماده۳۷ـ هنگام تفتیش رعایت موارد زیر ضروری است:

الف ـ شیوه اقدام نباید موجب تغییر، امحاء یا جابجایی داده‌های موردنظر در سامانه‌های رایانه‌ای باشد.

ب ـ تفتیش صرفاً در محدوده دستور قضایی و داده‌های مرتبط با جرم موضوع دستور، انجام می‌پذیرد.

ج ـ کلیه فرایندهای انجام شده بر روی داده‌های مورد تفتیش یا توقیف باید با استفاده از روش‌های قابل تشخیص، ثبت و محافظت شود.

ماده۳۸ـ توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود:

الف ـ در توقیف داده‌ها از طریق چاپ داده‌ها، غیرقابل دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذر واژه یا رمزنگاری و ضبط حامل‌های داده.

ب ـ در توقیف سامانه‌های رایانه‌ای یا مخابراتی از طریق تغییر گذرواژه، پلمب سامانه در محل استقرار یا ضبط سامانه.

تبصره ـ توقیف باید حتی‌الامکان بدون ایجاد مانع برای فعالیت سامانه و به روش ساده و کم هزینه به شیوه‌هایی از قبیل ذخیره در حامل‌های داده، ذخیره در سامانه با گذاشتن گذرواژه، تهیه نسخه پشتیبان، تصویربرداری، تهیه رونوشت و چاپ انجام شود.

ماده۳۹ـ دستور توقیف سامانه شامل سایر سخت‌افزارها یا حامل‌های داده متصل به آن نمی‌شود، مگر آن که در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت‌افزارها یا حامل‌های داده، ضابطان یا سایر مأموران در حدود وظایف قانونی می‌توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون و رعایت مقررات این آیین‌نامه اقدام نمایند.

ماده۴۰ـ در صورت پلمب سامانه چنانچه نیاز به گماردن حافظ باشد با دستور مقام قضایی اقدام می‌شود.

ماده۴۱ـ به منظور حفظ وضعیت اصلی ادله رایانه‌ای و جلوگیری از هرگونه تغییر، تحریف یا آسیب آن، مرجع قضایی مدت زمان نگهداری و مراقبت از آنها را تا مدت ۵ روز تعیین می‌کند.

تبصره ـ چنانچه برای نگهداری و مراقبت مدت بیشتری مورد نیاز باشد، مدت مذکور به صورت مستدل توسط مقام قضایی تمدید می‌شود.

ماده۴۲ـ اجرای دستور توقیف باید طی صورت‌جلسه‌ای با قید دقیق جزئیات و مشخصات داده یا سامانه، محل، تاریخ و زمان دقیق، مشخصات حاضران و مجری دستور، مشخصات حافظ در صورت وجود، شماره و تاریخ دستور قضایی مبنی بر توقیف، شیوه توقیف و مشخصات مالک یا متصرف داده یا سامانه و موارد ضروری دیگر تنظیم و ضمن اعلام به مقام قضایی رسیدگی‌کننده، در سابقه ضبط گردد.

ماده۴۳ـ ضابطان قضایی و سایر مأموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت وضعیت اولیه‌ای از سامانه رایانه‌ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت‌افزارها و حامل‌های داده متصل به آن که علامت‌گذاری و ثبت می‌شوند را تنظیم و به امضای تفتیش‌کننده یا توقیف‌کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم‌مقام قانونی وی برسانند. برای ضبط دقیق مشخصات ابزار و اجزای آن تصویربرداری بلامانع است.

ماده۴۴ـ مرجع قضایی صالح، ضمن صدور رأی باید نسبت به داده یا سامانه توقیف شده تعیین تکلیف نماید.

فصل سوم: امور متفرقه

ماده۴۵ـ دستورالعمل حقوقی و فنی جمع‌آوری ادله و توقیف سامانه‌های رایانه‌ای و مخابراتی توسط دادستانی کل کشور با همکاری نیروی انتظامی تهیه و به تصویب دادستان کل کشور می‌رسد. این دستورالعمل باید دربردارنده چگونگی حفظ صحنه جرم و جمع‌آوری ادله از سامانه در حال اجراء ، خاموش و روشن کردن سامانه، بسته‌بندی و انتقال اطلاعات و نیز نمونه درخواست‌های مرتبط با این موارد باشد.

ماده۴۶ـ در مورد جمع‌آوری ادله الکترونیکی از جمله نگهداری، حفظ فوری، تفتیش و توقیف و شنود چنانچه موضوع مربوط به افراد و اماکن وابسته به قوه قضائیه و سازمان‌های تابعه مراکز مرتبط با قوه قضاییه باشد، با دستور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضاییه انجام خواهد شد.

ماده۴۷ـ نسخه‌های تهیه شده از داده‌های رایانه‌ای قابل استناد به صورت متن، صوت یا تصویر در حکم اصل داده می‌باشند.

ماده۴۸ـ این آیین‌نامه توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ۴۸ ماده و ۱۱ تبصره در تاریخ ۱۳۹۳/۵/۱۲ به تصویب رئیس قوه قضائیه رسید.

رئیس قوه قضائیه ـ صادق آملی لاریجانی

۴۹۴۴

شماره۲۹۶/۲۹۴۴۲ ۱۳۹۳/۴/۳۱

حجت الاسلام والمسلمین جناب آقای دکتر حسن روحانی
ریاست محترم جمهوری اسلامی ایران

در اجرای اصل یکصد و بیست و سوم (۱۲۳) قانون اساسی جمهوری اسلامی ایران قانون تفسیر ماده (۱۳۳) قانون مالیاتهای مستقیم و اصلاحات بعدی آن که با عنوان طرح استفساریه به مجلس شورای اسلامی تقدیم گردیده بود، با تصویب در جلسه علنی روز سه‌شنبه مورخ ۱۳۹۳/۴/۱۷ و تأیید شورای محترم نگهبان، به پیوست ابلاغ می‌گردد.

رئیس مجلس شورای اسلامی ـ علی لاریجانی

شماره۵۱۱۳۴ ۱۳۹۳/۵/۱۱

وزارت امور اقتصادی و دارایی

در اجرای اصل یکصد و بیست و سوم قانون اساسی جمهوری اسلامی ایران «قانون تفسیر ماده (۱۳۳) قانون مالیات‌های مستقیم و اصلاحات بعدی آن» که در جلسه علنی روز سه‌شنبه مورخ هفدهم تیرماه یکهزار و سیصد و نود و سه مجلس شورای اسلامی تصویب و در تاریخ ۱۳۹۳/۴/۲۵ به تأیید شورای نگهبان رسیده و طی نامه شماره ۲۹۶/۲۹۴۴۲ مورخ ۱۳۹۳/۴/۳۱ مجلس شورای اسلامی واصل گردیده است، به پیوست جهت اجراء ابلاغ می‌گردد.

رئیس جمهور ـ حسن روحانی