آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی

در اجرای ماده ٥٤ 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

ماده ۱ ـ واژه‌ها و اصطلاحات به کار برده شده در این آیین‌نامه در معانی زیر به کار می‌رود:

الف) 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 تامین‌کنندگان، توزیع‌کنندگان، عرضه‌کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.

ب) ارائه‌دهندگان خدمات میزبانی: اشخاصی هستند که امکان دسترسی کاربران به فضای ایجادشده توسط سامانه‌های رایانه‌ای، مخابراتی و ارتباطی تحت تصرف یا کنترل خود را به کاربران واگذار می‌کنند تا راسا 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) ارائه داده‌های الکترونیکی: عبارت است از در اختیار قرار دادن تمام یا بخشی از

داده‌های حفظ یا نگهداری شده توسط ارائه‌دهندگان خدمات دسترسی یا میزبانی یا اشخاصی که داده‌ها را تحت تصرف یا کنترل دارند.

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

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

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

ز) مجری حفاظت: شخصی است که به نحوی داده‌های رایانه‌ای ذخیره‌شده را تحت تصرف یا کنترل دارد و مطابق ماده ۳٤ 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 به‌صورت 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 ارائه‌شده در قوانین دیگر می‌باشد.

فصل دوم: جمع‌آوری ادله الکترونیکی

مبحث اول: نگهداری داده‌ها

ماده ۲ـ ارائه‌دهندگان خدمات دسترسی و میزبانی موظف‌اند از سامانه‌هایی استفاده نمایند که قابلیت نگهداری داده‌های ترافیک و اطلاعات کاربران را مطابق مواد ۳۲ و ۳۳ قانون داشته باشد.

ماده ۳ـ ارائه‌دهندگان خدمات دسترسی موظف‌اند 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: عرضه‌کنندگان خدمات دسترسی حضوری اینترنت (کافی‌نت‌ها) موظف‌اند مشخصات هویتی، آدرس، ساعت شروع و خاتمه کار کاربر و نشانی اینترنتی (IP) تخصیصی را در دفتر روزانه ثبت نمایند.

ماده ٤ـ ارائه‌دهندگان خدمت دسترسی موظف‌اند اطلاعات کاربران را حداقل ٦ ماه پس از خاتمه اشتراک یا لغو قرارداد کاربر نگهداری کنند. هویت و نشانی کاربر باید در قرارداد منعقده درج شود.

ماده ۵ـ ارائه‌دهندگان خدمات میزبانی داخلی و نمایندگان داخلی ارائه‌دهندگان خدمات میزبانی خارجی موظف‌اند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره‌شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند. برگه اشتراک باید به نحوی تنظیم شود که هویت و نشانی آنان مشخص باشد.

تبصره ۱: ارائه‌دهندگان خدمات میزبانی موظف‌اند 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.

تبصره ۲: اشخاصی که نسبت به انباشت یا ذخیره موقت اطلاعات در راستای ارائه خدمات دسترسی اقدام می‌کنند، ارائه‌دهنده خدمات میزبانی محسوب نمی‌شوند.

ماده ٦ـ ارائه‌دهندگان خدمات دسترسی و میزبانی و مجریان حفاظت موظف‌اند امنیت داده‌های ترافیکی و محتوای نگهداری و حفاظت‌شده را مطابق با ضوابط و دستورالعمل‌هایی که به تصویب رئیس قوه قضائیه می‌رسد، تامین نمایند.

ماده ۷ـ 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.

ماده ۸ـ در مواردی که برابر قانون نگهداری و حفاظت داده‌ها الزامی است، نگهداری و حفاظت باید به گونه‌ای انجام شود که مدیریت جست‌وجو و گزارش‌دهی آنها امکان‌پذیر باشد.

ماده ۹ـ وزارت ارتباطات و فناوری اطلاعات هماهنگی‌های لازم برای تنظیم زمان سامانه‌های جمع‌آوری داده‌های محتوا، ترافیک و اطلاعات کاربران را مطابق با ساعت رسمی کشور به عمل می‌آورد.

ماده ۱۰ـ 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.

مبحث دوم: حفاظت از ادله رایانه‌ای

ماده ۱۱ـ مقام قضایی در جریان تحقیق و فرایند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره‌شده را از جمله داده‌های رمزنگاری‌شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده‌هایی که نوع و نام آنها موقتا تغییریافته و یا داده‌هایی که برای بررسی آنها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید.

تبصره۱: ضابطان قضایی فقط در موارد مندرج در ماده ۳٤ قانون می‌توانند راسا دستور حفاظت داده‌های ذخیره‌شده را صادر کنند.

تبصره۲: قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تایید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از

ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد.

ماده ۱۲ ـ دستور حفاظت باید به‌طور صریح و دقیق مشتمل بر نوع داده‌ها، موضوع و مدت‌زمان با رعایت تبصره ۲ ماده ۳٤ قانون، باشد.

ماده ۱۳ ـ در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می‌شود.

ماده ۱٤ ـ مجری حفاظت موظف است بلافاصله پس از ابلاغ، دستور حفاظت را اجرا 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.

ماده ۱۵ ـ دستور حفاظت باید فوری و با روش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشـــخاص ذی‌نفع نیز ابلاغ می‌شود؛ مگر آنکه ابلاغ به آنها مخلّ 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 مدت‌زمان حفاظت، امکان بهره‌برداری از داده‌های حفاظت‌شده را در مراحل بعدی دادرسی ممکن سازد.

ماده ۱٦ ـ حفاظت از داده‌ها باید به نحوی باشـــد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود.

مبحث سوم: ارائه ادله رایانه‌ای

ماده ۱۷ ـ دستور ارائه توسط مقام قضایی صادر می‌شود و باید به‌طور صریح و شفاف و مشتمل بر شخص ارائه‌دهنده، موضوع و نوع داده‌ها، شیوه و زمان تحویل داده‌ها و مرجع تحویل گیرنده باشد.

ماده ۱۸ ـ 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 کم‌هزینه به یکی از شیوه‌های ذیل باشد:

الف) تحویل یک نسخه چاپ‌شده از داده.

ب) تحویل یک نسخه رایانه‌ای از داده.

ج) ایجاد دسترسی به داده.

د) انتقال تجهیزات رایانه‌ای و مخابراتی.

ماده ۱۹ ـ هنگام ارائه داده‌ها صورت‌جلسه‌ای در سه نسخه تنظیم و حداقل موارد ذیل در آن ذکر و به امضای ارائه‌دهنده و تحویل گیرنده می‌رسد:

الف) شماره و تاریخ دستور قضایی ارائه داده‌ها

ب) مشخصات ارائه‌دهنده

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 به‌کاررفته در زمان ارائه

ح) مشخصات سخت‌افزاری و نرم‌افزاری تجهیزات

ط) شیوه ارائه و مشخصات داده.

تبصره ۱: در هنگام انتقال تجهیزات، احتیاط لازم برای حفظ آنها به عمل می‌آید.

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

ماده ۲۰ ـ از زمان ارائه داده‌ها به ضابطان قضایی یا دیگر اشخاص ذی‌ربط، مسئولیت حفظ داده‌های مذکور با شخص یا اشخاص تحویل گیرنده خواهد بود.

ماده ۲۱ ـ ارائه داده‌هایی که افشا یا دسترسی به آنها مطابق قوانین خاص دارای محدودیت یا توام با تشریفات می‌باشد، تابع مقررات مربوط است.

ماده ۲۲ ـ دستور ارائه داده، مجوز افشای آن نمی‌باشد و پس از دستور ارائه هرگونه دسترسی به مفاد داده مستلزم صدور دستور قضایی است.

ماده ۲۳ ـ اشخاصی که مسئول اجرای هر یک 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 یادشده هستند، حق افشای مفاد دستور و یا داده‌ها

و اطلاعات مربوط را ندارند.

د: تفتیش و توقیف ادله رایانه‌ای

ماده ۲۴ ـ 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) حتی‌الامکان نوع و میزان داده‌ها و سخت‌افزارها

ج) محل تفتیش یا توقیف

د) دلایل لازم برای تصویربرداری و بررسی در خارج از محل

هـ) زمان تقریبی لازم برای تفتیش و توقیف.

ماده ۲۵ ـ در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی‌الامکان در محل استقرار سامانه انجام پذیرد.

ماده ۲۶ ـ 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.

ماده ۲۷ ـ تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

ماده ۲۸ ـ 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 فورا به ذی‌نفع ابلاغ خواهد شد.

ماده ۲۹ ـ 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 ٤٤ قانون عمل می‌گردد.

ماده ۳۰ ـ قوه قضائیه 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.

ماده ۳۱ـ 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.

ماده ۳۲ـ رضایت متصرف قانونی سامانه موضوع بند ج ماده ٤١ قانون، باید کتبی و با امضای وی باشد.

ماده ۳۳ـ 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.

ماده ۳٤ـ ضابطان صرفا مجاز به تفتیش و توقیف داده‌ها و سامانه‌هایی هستند که به‌طور 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 امحا نسبت به حفظ فوری داده‌ها اقدام و مراتب را حداکثر ظرف ٢٤ ساعت کتبا به مقام قضایی مربوط گزارش می‌دهند.

ماده ۳۵ـ 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، و انکارناپذیری ادله انجام می‌پذیرد.

ماده ۳٦ـ 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.

ماده ۳۷ـ هنگام تفتیش رعایت موارد زیر ضروری است:

الف) شیوه اقدام نباید موجب تغییر، امحا یا جابجایی داده‌های مورد نظر در سامانه‌های رایانه‌ای باشد.

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

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

ماده ۳۸ـ توقیف با رعایت تناسب، نوع، اهمیت و نقش داده یا سامانه رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود:

الف) در توقیف داده‌ها از طریق چاپ داده‌ها، غیر قابل دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده.

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

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

ماده ۳۹ـ دستور توقیف سامانه شامل سایر سخت‌افزارها یا حامل‌های داده متصل به آن نمی‌شود، مگر آنکه در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت‌افزارها یا حامل‌های داده، ضابطان یا سایر ماموران در حدود وظایف قانونی می‌توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون و رعایت مقررات این آیین‌نامه اقدام نمایند.

ماده ۴۰ـ در صورت پلمب سامانه چنانچه نیاز به گماردن حافظ باشد با دستور مقام قضایی اقدام می‌شود.

ماده ۴۱ـ به‌منظور حفظ وضعیت اصلی ادله رایانه‌ای و جلوگیری از هرگونه تغییر، تحریف یا آسیب آن، مرجع قضایی مدت‌زمان نگهداری و مراقبت از آنها را تا مدت ۵

روز تعیین می‌کند.

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

ماده ٤٢ ـ 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.

ماده ٤٣ ـ ضابطان قضایی و سایر ماموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت‌وضعیت اولیه‌ای از سامانه رایانه‌ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت‌افزارها و حامل‌های داده متصل به آنکه 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.

ماده ٤٤ ـ مرجع قضایی صالح، ضمن صدور رای باید نسبت به داده یا سامانه توقیف‌شده تعیین تکلیف نماید.

فصل سوم: امور متفرقه

ماده ٤٥ ـ 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 اجرا، خاموش و روشن کردن سامانه، بسته‌بندی و انتقال اطلاعات و نیز نمونه درخواست‌های مرتبط با این موارد باشد.

ماده ٤٦ ـ 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 قضائیه باشـــد، با دســـتور مقام قضایی توسط مرکز حفاظت و اطلاعات قوه قضائیه انجام خواهد شد.

ماده ٤٧ ـ نسخه‌های تهیه‌شده از داده‌های رایانه‌ای قابل استناد به‌صورت متن، صوت یا تصویر در حکم اصل داده می‌باشند.

ماده ٤٨ ـ این آیین‌نامه توســـط وزارت دادگســـتری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و در ٤٨ ماده و ١١ تبصره به تصویب رئیس قوه قضائیه رسید.

رئیس قوه قضائیه ـ صادق آملی لاریجانی