وزارت نیرو
کارگروه تخصصی امنیت سایبری

الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو

(Geospatial Information Technology Security Requirements)

نوع مدرک: روش اجرایی **شناسه:** ECS-MOE-G-PR-GISSecurityReq-V1.0

نسخه: ۱.۰ **طبقه‌بندی:** داخلی **تاریخ آخرین اصلاح:** ۱۴۰۰/۰۲/۱۸

	تهیه	بازنگری	تایید و تصویب
رکن نظام‌نامه	کارگروه فناوری اطلاعات مکانی وزارت نیرو	کارگروه خدمات تخصصی امنیت سایبری	کارگروه تخصصی امنیت سایبری وزارت نیرو
سمت	دبیر کارگروه	رئیس کارگروه	رئیس کارگروه
نام	مهنام فلاح	دولت جمشیدی	ازرم دهستانی منفرد
تاریخ	۱۴۰۰/۴/۳	۱۴۰۰/۴/۳	۱۴۰۰/۴/۳
امضا			

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

جدول سوابق

شماره نسخه	تاریخ بازنگری	شرح تغییرات
۱.۰	۱۴۰۰/۰۲/۱۸	تهیه و تصویب

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

فهرست مطالب

عنوان — صفحه

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

۱- هدف و دامنه کاربرد

هدف از سند حاضر، متمرکزسازی الزامات و سیاست‌های امنیتی در حوزه فناوری اطلاعات مکانی است تا ضمن تسهیل امر تبادل داده و اطلاعات مکانی و به اشتراک‌گذاری آن، مخاطرات و تهدیدات سایبری، کنترل شده و کاهش یابند. بدین منظور در این سند، الزامات امنیتی که باید در طول چرخه حیات یک قلم داده مکانی موردتوجه قرار گیرند جهت رعایت در کلیه سامانه‌ها، ابزارها و بسترهای استفاده‌کننده از اطلاعات مکانی ارائه شده است. این سند یکی از اسناد حوزه امنیت فناوری اطلاعات است که توسط کارگروه تخصصی امنیت سایبری وزارت نیرو است.

دامنه کاربرد این الزامات حوزه ستادی وزارت نیرو، شرکت‌های مادرتخصصی، شرکت‌های زیرمجموعه و مراکز و مؤسسه‌های آموزشی و پژوهشی وابسته به وزارت نیرو بوده و شامل کلیه زیرساخت‌های صنعتی و فناوری اطلاعات و ارتباطات می‌باشد.

۲- مراجع و اسناد مرتبط

- آیین‌نامه اجرایی حفاظت از اسناد و اطلاعات طبقه‌بندی‌شده، شورای عالی امنیت ملی، ابلاغ شده توسط حراست وزارت نیرو
- نظام‌نامه امنیت سایبری وزارت نیرو، ۱۳۹۹
- سند چشم‌انداز و برنامه راهبردی فناوری اطلاعات مکانی وزارت نیرو، ۱۳۹۹
- https://www.ogc.org/standards/security
- https://www.stigviewer.com/stigs
- https://www.cisecurity.org/cis-benchmarks/
- https://owasp.org/www-project-web-security-testing-guide/
- https://cheatsheetseries.owasp.org/index.html
- Gertz Michael, Jajodia Sushil, "HandBook of Database Security, Applications and Trends", Springer, 2008.
- Bertino Elisa, Gertz Michael, "Security and Privacy for Geospatial Data: Concepts and Research Directions", International Workshop on Security and Privacy in GIS and LBS, 2008.
- Scott A. Bryant, "Geospatial Information Security Risks and Concerns of the United States Air Force Geobase Program" [Master's thesis, Department of the Air Force, Air University], 2007.

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

- Mohammd A. Bashir, "Geospatial Digital Rights Management with focus on Digital Licensing of GML datasets" [Master's thesis, International Institute for Geo-Information Science and Earth Observation], 2006.
- Wan Xiaogao, "Security of Geographic Information System", [Master's thesis, Politecnico di Milano], 2013.
- "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns", National Spatial Data Infrastructure (Program: U.S.), 2005.
- Hanashima Makoto, "Consideration for Information Security Issues in Geospatial Information Services of Local Governments", IASSIST Quarterly Winter, 2006.
- Hutter David, "Physical Security and Why It Is Important", SANS Institute, 2016.
- Jon S. Warner, Roger G. Johnston, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing", The Journal of Security Administration, 2012.
- Kissel Richard, Regenscheid, "Guidelines for Media Sanitization", NIST Special Publication 800-88 1, 2016.
- Burney Aqil, Asif Muhammad, "Google Maps Security Concerns", Journal of Computer and Communications, 2018.

۳- تعاریف

حوزه‌های سه‌گانه وزارت نیرو: حوزه ستادی برابر با سطح یک (سطح حاکمیتی)، شرکت‌های مادر تخصصی و ساتبا برابر با سطح دو (سطح تخصصی- میانی)، شرکت‌های زیرمجموعه شرکت‌های مادر تخصصی (منطقه‌ای یا استانی) و مراکز و موسسه‌های آموزشی و پژوهشی وابسته به وزارت نیرو برابر با سطح سه (سطح عملیاتی) می‌باشند.

داده مکانی: هر نوع داده‌ای که شامل اطلاعات یک مکان همانند آدرس یک نقطه، کد پستی یک مکان، مختصات جغرافیایی یک رودخانه، محل خطوط انتقال آب، مختصات یک پست برق و غیره باشد، داده مکانی[1] محسوب می‌شود.

شیء مکانی: یک شیء قابل‌تشخیص که در یک محل مشخص با مختصات جغرافیایی منحصربه‌فرد قرار گرفته باشد، شیءمکانی[2] نام دارد. دکل، پست برق، سد، تصفیه‌خانه، خط انتقال آب، رودخانه و غیره نمونه‌ای از این اشیاء هستند. هر شیءمکانی به کمک ویژگی‌هایی مانند طول و عرض جغرافیایی، ارتفاع، پهنا، تاریخ و زمان ثبت اطلاعات مربوطه و همچنین ویژگی‌های مکانی توصیف می‌شود.

سامانه اطلاعات مکانی: سامانه اطلاعات مکانی یا GIS[3] چارچوبی برای جمع‌آوری، ذخیره‌سازی، بازیابی، پردازش، آنالیز و نمایش داده‌های مکانی است. سامانه اطلاعات مکانی می‌تواند در بسترهای دسکتاپ، تحت وب یا موبایل پیاده‌سازی شده و مورد استفاده قرار گیرد.

زیرساخت داده‌های مکانی: به چارچوبی از فناوری‌ها، سیاست‌ها و قراردادهای سازمانی که برای ایجاد، تبادل و استفاده از داده‌های مکانی در فضای به اشتراک‌گذاری اطلاعات به کار می‌روند، زیرساخت داده‌های مکانی یا SDI[4] گفته می‌شود. این چارچوب، امکان به اشتراک‌گذاری اطلاعات مکانی را در سطح یک سازمان و یا حتی در سطوح ملی و بین‌المللی فراهم می‌کند. در تمام این موارد SDI باید قابلیت ارسال، جستجو، ارزیابی و تبادل اطلاعات مکانی را به‌صورت خودکار و در چارچوب قراردادهای سازمانی، برای تأمین‌کنندگان و مصرف‌کنندگان اطلاعات فراهم کند.

Map Server: سرویس‌دهنده‌ای که با استفاده از داده‌های مکانی ذخیره‌شده در یک پایگاه داده GIS، امکان استفاده از نقشه‌ها را بر روی وب فراهم می‌کند، Map Server نامیده می‌شود. درواقع این سرویس‌دهنده‌ها، امکان بصری‌سازی داده‌های نقشه و اطلاعات جغرافیایی را برای کلاینت‌های خود فراهم می‌کنند.[5]

---

[1] Geospatial Data
[2] Spatial Object
[3] Geospatial Information System
[4] Spatial Data Infrastructure
[5] jghg

OGC Services: سازمان OGC[1] استانداردهای موردنیاز برای دسترسی، نمایش و پردازش داده‌های مکانی را در قالب مجموعه‌ای از سرویس‌های وب تعریف کرده است که به آن‌ها OWS[2] گفته می‌شود. WMS[3]، WFS[4] و WCS[5] نمونه‌ای از این سرویس‌ها هستند. درخواست‌های OWS به کمک پروتکل HTTP[6] تعریف و به کمک ساختارهایی همانند XML[7] کدگذاری می‌شوند.

چرخه حیات داده‌های مکانی: چرخه حیات داده‌های مکانی، توالی مراحلی است که یک واحد از داده‌ها از تولد تا مرگ خود طی می‌کند. این مراحل شامل تولید، ذخیره‌سازی، پردازش و استفاده، به اشتراک‌گذاری، آرشیو و حذف است.

اولویت اقدام: اولویت مشخص‌شده برای اجرا و اعمال هر یک از اقدامات موردنیاز که بر اساس شرایط و امکانات موجود شرکت‌های صنعت آب و برق مشخص شده است. اولویت اقدام ۱ به معنای بالاترین اولویت و اولویت اقدام ۳ به معنای پایین‌ترین اولویت است.

۴- مسئولیت

مسئولیت تصویب و ابلاغ این روش اجرایی بر عهده کارگروه تخصصی امنیت سایبری وزارت نیرو است.

مسئولیت اجرا در حوزه ستادی وزارت نیرو بر عهده مدیرکل دفتر فناوری اطلاعات و آمار، در شرکت‌های مادر تخصصی و ساتبا بر عهده معاون ذی‌ربط و در شرکت‌های زیرمجموعه بر عهده مدیرعامل و در مراکز و موسسه‌ها بر عهده رؤسای آن‌هاست.

مسئولیت نظارت بر چگونگی اجرای این سند در هر شرکت بر عهده کارگروه تخصصی امنیت مربوطه و با حضور واحدهای حراست است. نظارت عالیه بر سند بر عهده مرکز حراست وزارت نیرو است.

[1] Open Geospatial Consortium
[2] OGC Web Service
[3] Web Map Service
[4] Web Feature Service
[5] Web Coverage Service
[6] Hypertext Transfer Protocol
[7] Extensible Markup Language

۵- تشریح الزامات و روش اجرا

در این بخش فهرست الزامات امنیتی در حوزه فناوری اطلاعات مکانی به همراه الویت اجرای آنها مشخص شده است. برای این منظور ابتدا وظایف واحدهای GIS در قالب ساختار اجرایی (بخش ۵-۱) بیان شده است. سپس تعریف انواع کاربران و حقوق دسترسی آنها به داده‌های مکانی در بخش ۵-۲ آورده شده است. در نهایت فهرست تمام الزامات امنیتی داده‌های مکانی در طول چرخه حیات آنها در بخش ۵-۳ بیان شده است.

۵-۱- ساختار اجرایی

واحدهای GIS در کلیه شرکت‌های تابعه موظف‌اند ظرف مدت ۶ ماه از ابلاغ سند، اقدامات زیر را اجرایی نمایند:

- نسبت به شناسایی و مستندسازی اطلاعات مرتبط با فناوری اطلاعات مکانی در سازمان متبوع خود شامل موارد زیر اقدام کرده و آن را در قالب یک سند مرجع تدوین و به‌روزرسانی نمایند:
- شناسنامه و فراداده[1] کلیه داده‌های مکانی مورداستفاده در سازمان
- مشخصات فنی کلیه سامانه‌های نرم‌افزاری دسکتاپ، تحت وب و موبایل که به هر نحو داده‌های مکانی را تولید، ذخیره‌سازی و یا پردازش می‌کنند؛ شامل سامانه GIS و یا سایر سامانه‌های عملیاتی مانند بهره‌برداری، حقوقی، مهندسی و غیره
- اقدامات مشخص‌شده در مفاد سند را که به‌عنوان اولویت اقدام ۱ تعیین‌شده‌اند، بر روی کلیه موارد شناسایی‌شده بند قبل، اجرا و پیاده‌سازی نمایند (اولویت‌های ۲ و ۳ به‌منزله موارد اختیاری بوده و در ارزیابی‌های مرحله اول لحاظ نخواهند شد).
- کلیه قراردادهای مرتبط با داده‌ها و سامانه‌های مکانی جاری شرکت را به لحاظ رعایت مفاد این سند بررسی کرده و اصلاحات لازم را به پیمانکار مربوطه ابلاغ نمایند. همچنین اجرا و رعایت آن‌ها را در قراردادهای در حال انعقاد و آتی الزامی نمایند.
- کاربران استفاده‌کننده از داده‌ها، نرم‌افزارها و دستگاه‌های همراه مکانی را نسبت به روش‌های واگذاری اطلاعات و مخاطرات آن آگاه کنند و آموزش‌های لازم را در سطوح مختلف ارائه دهند.
- واحدهای فناوری اطلاعات در کلیه شرکت‌های تابعه موظف‌اند همکاری لازم را در اجرای مفاد سند با واحدهای GIS به عمل آورند.

وزارت نیرو
کارگروه تخصصی امنیت سایبری

[1] فراداده، نقشه‌ها، فایل‌های GIS و دیگر منابع داده‌ای مبتنی بر مکان را توصیف می‌کند.

واحدهای حراست در کلیه شرکت‌های تابعه موظف‌اند در راستای موارد زیر اقدام نمایند:

- انعقاد قرارداد عدم افشای اطلاعات و حفظ محرمانگی با تمامی افراد داخل و خارج سازمان و شرکت‌های طرف قرارداد که با داده‌ها یا نرم‌افزارهای مکانی مرتبط هستند.
- بررسی و تائید صلاحیت امنیتی شرکت‌های طرف قرارداد مرتبط با داده‌ها یا نرم‌افزارهای مکانی.
- استفاده از کنترل‌های امنیتی فیزیکی همانند کارت‌های هوشمند، سامانه‌های نظارتی مجهز به دوربین‌های با کیفیت بالا، حفاظ‌ها و گیت‌های مجهز به مکانیسم‌های تشخیص حرکت و هویت در نواحی مراکز داده‌های مکانی.
- مطابق با تعریف ارائه‌شده از «اسناد طبقه‌بندی‌شده» در «آیین‌نامه اجرایی حفاظت از اسناد و اطلاعات طبقه‌بندی‌شده» ابلاغ‌شده از سوی مرکز حراست وزارت نیرو، که به تصویب دبیر وقت شورای عالی امنیت ملی رسیده است، داده‌های مکانی جزو اسناد طبقه‌بندی‌شده محسوب نمی‌گردد؛ لذا جهت تبادل امن آن‌ها در رویه‌های اجرایی مطلوب، صرفاً استناد به مفاد سند حاضر الزامی است.
- تبادل داده و اطلاعات مکانی در مجموعه وزارت نیرو (فی‌مابین هر سه سطح و بین شرکت‌های مادرتخصصی) با رعایت موارد مندرج در سند حاضر بلامانع است و نیازی به اخذ مجوز جداگانه از سایر نهادها و واحدها نیست.
- واگذاری اطلاعات به متقاضیان دولتی خارج از مجموعه وزارت نیرو، شهرداری‌ها، دانشگاه‌ها و مؤسسات علمی-پژوهشی و یا عقد هرگونه تفاهم‌نامه با آن‌ها جهت واگذاری اطلاعات در شرایط بحران و اضطرار و یا جهت پاسخگویی به استعلامات الکترونیکی، مطابق با مفاد سند و پس از تائید در کارگروه تخصصی امنیت شرکت امکان‌پذیر است.

۲-۵- مدیریت کاربران و داده‌های مکانی

در این بخش با توجه به ضرورت تعیین نحوه برخورد با داده‌های مکانی در مجموعه وزارت نیرو، کاربران، انواع دسترسی‌ها و طبقه‌بندی استاندارد داده‌ها بیان شده است.

- شرکت‌های سطح دو وزارت نیرو موظف‌اند حداکثر ظرف مدت ۶ ماه از ابلاغ سند حاضر، برای کلیه داده‌های مکانی حوزه تحت پوشش خود سند «طبقه‌بندی محرمانگی داده، اطلاعات و سرویس» را تدوین کرده و جهت اعمال و رعایت به شرکت‌های تابعه ابلاغ نمایند.
- کلیه شرکت‌های تابعه وزارت نیرو موظف‌اند مطابق انواع کاربران (جدول ۱) و حقوق دسترسی (جدول ۲)، نسبت به تعیین نقش‌های کاربری و اعطای حق دسترسی لازم برای هر نوع کاربر (جدول ۳)، در کلیه سامانه‌های شرکت که از داده‌های مکانی استفاده می‌کنند اقدام نمایند.

وزارت نیرو
کارگروه تخصصی
امنیت سایبری

جدول ۱- انواع کاربران

ردیف	کاربر	توضیح
۱	سازمانی	کاربران حقیقی داخل سازمان که می‌بایست بر اساس واحد و وظایف سازمانی، در نقش‌های مختلف دسته‌بندی شوند؛ مانند متخصصین GIS که به‌صورت تخصصی با داده‌ها و ابزارهای مکانی سروکار دارند، کارشناسان و مدیران سازمان که از داده‌ها و تحلیل‌های مکانی طی فرآیندهای کاری خود استفاده می‌کنند و یا در رویه‌های مشخص در به‌روزرسانی یا اعتبارسنجی داده‌ها مشارکت دارند.
۲	فرا سازمانی	کاربران حقیقی یا حقوقی خارج از سازمان که از شرکت‌های زیرمجموعه وزارت نیرو (شامل کلیه شرکت‌های سطح یک، دو و سه) هستند.
۳	خارجی	کاربران حقیقی یا حقوقی خارج از سازمان که از نهادهای خارج از مجموعه وزارت نیرو مانند شهرداری‌ها، استانداری‌ها، سازمان‌های خدماتی و غیره هستند.
۴	مجری	شرکت‌های پیمانکار یا مشاور طرف قرارداد با سازمان و دارای مجوز که تأییدیه لازم را از واحد حراست اخذ کرده‌اند و در حوزه توسعه و پشتیبانی سامانه GIS، برداشت و ورود داده‌های مکانی و یا توسعه سرویس‌های تبادل داده مکانی در سایر سامانه‌های سازمان فعالیت می‌کنند.

جدول ۲- انواع حقوق دسترسی

ردیف	حق دسترسی	توضیح
۱	مشاهده	مشاهده داده‌ها و اطلاعات مرتبط، بزرگنمایی و پیمایش از وضوح کم به بالا، به‌صورت مستقیم، از طریق سرویس یا خروجی‌های تصویری فیزیکی
۲	ویرایش	عملکرد درج یا ورود داده جدید، حذف، ویرایش، اصلاح و به‌روزرسانی داده‌ها به‌صورت مستقیم یا از طریق سرویس
۳	تحلیل	آنالیز روی داده‌های مکانی و استفاده از ابزارهای پردازشی به‌صورت مستقیم یا از طریق سرویس
۴	ذخیره	استخراج، دریافت و ذخیره داده‌ها در محلی خارج از سامانه سازمانی با فرمت‌های برداری و قابل‌تحلیل به‌صورت مستقیم یا از طریق سرویس
۵	مدیریت	مدیریت کاربران، نقش‌ها و سطوح دسترسی به لایه‌ها و ابزارها

جدول ۳-حقوق دسترسی به تفکیک انواع کاربران

ردیف	انواع کاربر	حقوق دسترسی				
		مشاهده	ویرایش	تحلیل	ذخیره	مدیریت
۱	سازمانی	متناسب با حوزه کاری	متناسب با نقش	متناسب با نقش	متناسب با نقش و با اعمال محدودیت	متناسب با نقش
۲	فرا سازمانی	متناسب با کاربرد	-	-	صرفاً تحت شرایط ویژه	-
۳	خارجی	در محدوده تفاهم‌نامه	-	-	-	-
۴	مجری	در محدوده قرارداد	در محدوده قرارداد	در محدوده قرارداد	-	-

۳-۵- الزامات چرخه حیات داده‌های مکانی

در این بخش کلیه الزامات امنیتی مبتنی بر فازهای مختلف چرخه حیات داده‌های مکانی دسته‌بندی و ارائه‌شده‌اند.

۱-۳-۵- تولید، برداشت و جمع‌آوری داده‌های مکانی

واحدهای GIS کلیه شرکت‌های تابعه مسئولیت اجرا و نظارت بر تولید، برداشت و جمع‌آوری داده‌های مکانی را (از طریق مجری/مشاور/پیمانکار مربوطه) بر عهده‌دارند. همچنین موظف‌اند متناسب با روش برداشت موردنظر، الزامات جدول ۴ را در پیوست قراردادهای برداشت و جمع‌آوری اطلاعات مکانی لحاظ کنند.

جدول ٤- الزامات امنیتی تولید، برداشت و جمع‌آوری داده‌های مکانی

ردیف	روش و ابزار برداشت	الزام	اولویت اقدام
۱	دوربین‌های نقشه‌برداری، گیرنده‌های GNSS[1] (استاتیک و RTK[2])، سنجنده‌های مورداستفاده برای برداشت اطلاعات زیرسطحی مانند GPR[3] و غیره، دستگاه‌های موردنیاز برای برداشت اطلاعات نقشه‌های هیدروگرافی مانند اکوساندر و غیره	در زمان تخلیه اطلاعات، چنانچه امکان ارسال اطلاعات جمع‌آوری‌شده توسط دستگاه به سرور اصلی از طریق شبکه وجود نداشته باشد اتصال و تخلیه اطلاعات دستگاه می‌بایست تنها بر روی یک کامپیوتر مجاز در سازمان صورت گیرد.	۱
۲	دستگاه‌های همراه (موبایل، تبلت)	رعایت کلیه الزامات مندرج در بخش ۵-۲-۳ (پردازش و استفاده از داده‌های مکانی) در نرم‌افزار همراه مربوطه	۱
۳	پهپاد (UAV[4]) و دوربین‌های عکاسی	- انعقاد قرارداد فقط با مشاوران دارای صلاحیت برداشت داده با پهپاد[5] - اخذ مجوزهای رسمی لازم از مراجع ذیصلاح (نظامی/امنیتی) - نظارت نماینده GIS در زمان پرواز، تخلیه و پردازش اطلاعات	۱
۴	سنسورهای LiDAR[6]	با توجه به وجود افزونگی داده در داده‌های LiDAR لازم است: - فیلترگذاری‌های لازم بر روی داده خام اعمال شود تا فقط داده‌های موردنیاز استخراج‌شده و در پایگاه داده ذخیره گردند. - داده‌ها می‌بایست صرفاً پس از پردازش و تولید عوارض موردنیاز در قالب نقشه و با فرمت‌های معمول برداری، در اختیار کاربران قرار گیرد.	۱

[1] Global Navigation Satellite System
[2] Real-time kinematic positioning
[3] Ground-penetrating radar
[4] Unmanned Aerial Vehicle
[5] صلاحیت مشاوران، توسط سازمان نقشه برداری کشور و براساس آیین نامه ها و دستورالعمل های آن سازمان تعیین و احراز می گردد.
[6] Light Detection and Ranging

ردیف	روش و ابزار برداشت	الزام	اولویت اقدام
		نگهداری داده‌ها در فرمت‌های متعارف ابر نقطه[1] مانند las.	۱
		اطمینان از عدم اتصال به اینترنت تا زمان تخلیه اطلاعات در صورت استفاده از تلفن‌های همراه دارای سنسور LiDAR	۱

۲-۳-۵- ذخیره‌سازی داده‌های مکانی

رعایت الزامات امنیتی در راستای تأمین امنیت نرم‌افزارهای مدیریت پایگاه داده مکانی (جدول ۵)، سرورهای GIS (جدول ۶) و آرشیو و پشتیبان‌گیری از داده‌های مکانی (جدول ۷)، در کلیه شرکت‌های تابعه وزارت نیرو الزامی است.

جدول ۵- الزامات امنیتی نرم‌افزارهای مدیریت پایگاه داده مکانی

ردیف	الزام	اولویت اقدام
۱	امن‌سازی سیستم مدیریت پایگاه داده بر اساس چک‌لیست‌های موجود سازمان و مبتنی بر منابعی همانند چک‌لیست‌های اختصاصی شرکت‌های اصلی ارائه‌دهندگان محصول و چک‌لیست‌های CIS[2]، STIG[3]	۱
۲	استفاده از مکانیسم‌های حفاظتی مانند Firewall پایگاه داده‌ها و پراکسی معکوس برای حفاظت از درخواست‌های ارسالی به سرویس‌دهنده پایگاه داده‌ها در برابر حملاتی همانند SQL Injection و جلوگیری از نشت اطلاعات در پاسخ‌های تولیدشده	۳
۳	مدیریت متمرکز کلیه دسترسی‌ها (مطابق جدول ۴) به پایگاه داده، توسط راهبر سیستم مدیریت پایگاه داده	۱
۴	رمزنگاری[4] داده‌های مکانی حساس موجود در پایگاه داده‌ها با استفاده از روش‌هایی همانند TDE[5]، رمزنگاری قابل جستجو (SE[6]) و رمزنگاری لایه‌ای و یا استفاده از مکانیسم برچسب‌گذاری[7] داده‌ها و انواع رویکردها با سطوح مختلف ریزدانگی مثلاً در سطح فیلد	۲

جدول ٦- الزامات امنیتی سرورهای GIS

ردیف	الزام	اولویت اقدام
۱	امن‌سازی سرورهای وب‌اپلیکیشن و GIS بر اساس چک‌لیست‌های موجود سازمان و مبتنی بر منابعی همانند چک‌لیست‌های اختصاصی شرکت‌های اصلی ارائه‌دهندگان محصول و چک‌لیست‌های CIS، STIG	۱
۲	غیرفعال‌سازی اکانت‌های کاربری پیش‌فرض Guest و Administrator در سیستم‌عامل سرورهای GIS و تعریف و استفاده از اکانت‌های اختصاصی به راهبر سرور	۱
۳	به‌روزرسانی مستمر سیستم عامل سرورهای GIS و نصب آخرین وصله‌های امنیتی روی آن‌ها	۱

[1] ابر نقطه (Point Cloud) مجموعه‌ای از نقاط داده‌ای در فضا هستند که یک شیء یا شکل سه بعدی را توصیف می‌کنند. این نقاط توسط تکنولوژی‌هایی همانند LiDAR تولید می‌شوند.

[2] Center for Internet Security
[3] Security Technical Implementation Guide
[4] Encryption
[5] Transparent Data Encryption
[6] Searchable Encryption
[7] Labeling

ردیف	الزام	اولویت اقدام
۴	فعال‌سازی آنتی‌ویروس‌ها و آنتی‌باج‌افزارهای بروز شده با License معتبر بر روی سرورهای GIS	۱
۵	ایجاد افزونگی [1] در انواع مؤلفه‌های زیرساخت ذخیره‌سازی و پردازش داده‌ها با بهره‌گیری از معماری چند ماشینی [2] در هر یک از سرورها، توزیع عملکرد سرور بین چند ماشین و استفاده از پراکسی معکوس [3] برای توازن بار بین سرورهای Back-end در GIS برای تأمین دسترس‌پذیری بالا (HA[4]) به داده‌ها و مقابله با تهدید Single Point Of Failure با توجه به ریسک عدم تأمین سرویس (در این صورت سرور وب‌اپلیکیشن، درخواست‌های کلاینت را باید به این پراکسی ارسال کند).	۳
۶	مجزا کردن سرورهای (ماشین‌های مجازی) نقشه، وب‌اپلیکیشن و پایگاه داده‌ها از یکدیگر و رعایت این نکته که سرور پایگاه‌داده‌ها نباید در ناحیه DMZ [5] باشد.	۱
۷	استفاده از مکانیسم‌های حفاظتی مانند Firewall وب‌اپلیکیشن (WAF[6]) برای کنترل و آنالیز ترافیک پروتکل‌های HTTP و HTTPS که به وب‌اپلیکیشن وارد یا از آن خارج می‌شوند	۲
۸	تهیه و تحلیل مستمر گزارش‌های حوادث و خرابی‌های سرورهای GIS	۱

جدول ۷- الزامات آرشیو و پشتیبان‌گیری از داده‌های مکانی

ردیف	الزام	اولویت اقدام
۱	پیاده‌سازی خط‌مشی تهیه نسخه‌های پشتیبان از داده‌ها (مطابق دستورالعمل مصوب کمیته تخصصی امنیت شرکت‌های مادر تخصصی) شامل تعداد نسخ پشتیبان و محل ذخیره‌سازی آن‌ها، روش پشتیبان‌گیری، نحوه دسترسی و همچنین مدت‌زمان نگهداری نسخه‌ها	۱
۲	استفاده از راهکارهای مدیریت دارایی‌های دیجیتال (DAM)[7] برای آرشیوها	۳
۳	استفاده از الگوریتم‌های رمزنگاری مورد تائید سازمان برای حفاظت از آرشیوها	۳
۴	ذخیره و نگهداری نسخه‌های پشتیبان داده‌ها در محل‌های فیزیکی یا مجازی مستقل از محل ذخیره‌سازی داده‌های اصلی	۱
۵	انجام بررسی‌های لازم به‌صورت دستی یا به کمک مکانیسم‌هایی مانند Checksum پس از عملیات پشتیبان‌گیری، برای اطمینان از یکسان بودن تاریخ، اندازه و محتوای نسخه اصلی و پشتیبان	۳

۳-۳-۵- پردازش و استفاده از داده‌های مکانی

- کلیه شرکت‌های تابعه موظف‌اند برای توسعه، پیاده‌سازی و استفاده از سامانه‌های مکانی به فهرست ابزارها و نرم‌افزارهای تجاری و نرم‌افزارهای متن‌بازی که به تائید کمیته امنیت وزارت نیرو رسیده است مراجعه کرده و

---

[1] Redundancy
[2] Multi-Machine Architecture
[3] Reverse Proxy
[4] High Availability
[5] Demilitarized Zone
[6] Web Application Firewall
[7] پلتفرم‌ها و ابزارهای DAM (Digital Asset Management) امکان آرشیو انواع فایل‌ها اعم از مستندات متنی، تصاویر و غیره و همچنین مدیریت دسترسی به آنها را به صورت متمرکز فراهم می‌کنند.

استفاده از آن‌ها را در قراردادهای توسعه نرم‌افزار اعمال نمایند[1]. ابزارها و موارد جدید پس از طرح در کمیته امنیت و اخذ تائید به فهرست مذکور اضافه می‌گردند.

- در راستای استفاده امن از سامانه‌های مکانی، رعایت موارد مندرج در جدول ۸ و جدول ۹، و جهت امن سازی دستگاه‌های کاربران استفاده‌کننده از سامانه‌ها، رعایت موارد مندرج در جدول ۱۰ الزامی است.

جدول ۸- استفاده امن از سامانه‌های مکانی

ردیف	الزام	اولویت اقدام
۱	تعریف و ارزیابی سیاست‌های کنترل دسترسی به داده‌های مکانی با استفاده از مکانیسم کنترل دسترسی فراهم‌شده توسط سامانه‌های مکانی و مدل مجازشماری[2] آن	۱
۲	رعایت اصل اعطای حداقل مجوز موردنیاز[3] به نقش‌های کاربری	۱
۳	نظارت مداوم بر اکانت‌های کاربری تعریف‌شده و منقضی کردن اکانت افرادی که سازمان را ترک کرده‌اند.	۱
۴	فراهم کردن امکان پیاده‌سازی Proxy Page با قابلیت محدودسازی اتصال به آن بر روی دامنه یا IP و جلوگیری از حملات DoS[4] و DDoS[5] در سطح اپلیکیشن و Proxy Page[6]	۱
۵	جهت تأمین نقشه‌های پایه در نرم‌افزارها و سامانه‌های مکانی: - اولویت با استفاده از سرویس‌های نقشه بومی است. در صورت تأمین نشدن نیاز سازمان و استفاده از سرویس‌های نقشه غیربومی همانند Google Maps, Google Earth، Bing Maps، OSM[7] می‌بایست Tileهای محدوده تحت پوشش شرکت دانلود و در سرور داخلی شرکت بارگذاری گردد تا به‌صورت آفلاین مورداستفاده قرار گیرند. - در دستگاه‌های همراه، قبل از شروع عملیات در محل، نقشه‌ها در حافظه دستگاه کش شده و به‌صورت آفلاین مورداستفاده قرار گیرند.	۱
۶	به دلیل ناشناخته بودن و عدم امکان اعمال محدودیت دسترسی در ابزارهایی مانند Google Earth: - واحدهای GIS موظف‌اند ابزارها و قابلیت‌های لازم برای مشاهده و استفاده از داده‌های مکانی با فرمت‌های موردنیاز واحدهای کسب‌وکار را در سامانه‌های مکانی داخلی شرکت فراهم کنند. - داده‌ها و نقشه‌های GIS نباید در فضاهای مذکور به‌صورت مستقیم بارگذاری یا استفاده گردند. در صورت الزام به استفاده از ابزار Google Earth، لازم است داده‌های موردنظر صرفاً در قالب سرویس مکانی Publish شده و سپس در نرم‌افزار مذکور استفاده شوند.	۱

[1] فهرست مذکور در پایگاه اینترنتی فناوری اطلاعات مکانی وزارت نیرو به آدرس https://git.moe.gov.ir در دسترس است.

[2] Authorization

[3] Least Privilege Principle

[4] Denial of Service

[5] Distributed Denial of Service

[6] با توجه به ضرورت استفاده از دو Webserver جداگانه در سامانه‌های مکانی، به علت وجود Map server ها، استفاده از Proxy Page ضروری است.

[7] Open Street Map

جدول ۹- استفاده امن از سامانه‌های مکانی همراه

ردیف	الزام	اولویت اقدام
۱	اخذ تعهد لازم از کاربران مربوطه مبنی بر عدم دست‌کاری نرم‌افزاری و سخت‌افزاری دستگاه	۱
۲	عدم نصب و استفاده از نرم‌افزارهایی که Source آن‌ها در دسترس نیست بر روی دستگاه‌های همراه سازمانی	۱
۳	کاربر نباید از سیم‌کارت جدیدی که خارج از سرویس APN[1] اختصاصی است بر روی دستگاه‌های همراه سازمانی استفاده کند و همچنین نباید به هیچ شبکه بی‌سیم دیگری متصل شود.	۱
۴	در موارد ضروری که استفاده از سیم‌کارت APN بر روی دستگاه‌های همراه شخصی و غیرسازمانی مقدور نیست، استفاده از نرم‌افزار مطابق با حقوق دسترسی کاربران در جدول ۴ و صرفاً از طریق اتصال به شبکه VPN[2] فراهم شود.	۱
۵	داده‌ها و لایه‌های مکانی برای نمایش و استفاده روی بستر موبایل، صرفاً بر اساس ضرورت و کاربرد انتخاب‌شده و از نمایش لایه‌های غیرضروری اجتناب گردد.	۱
۶	چنانچه امکان ارسال اطلاعات جمع‌آوری‌شده توسط دستگاه به سرور اصلی از طریق شبکه وجود نداشته باشد اتصال و تخلیه اطلاعات دستگاه می‌بایست تنها بر روی یک کامپیوتر مجاز در سازمان صورت گیرد.	۱
۷	اعلام مفقودی یا سرقت دستگاه، حداکثر ظرف ۲۴ ساعت به واحد حراست	۱
۸	تحویل‌گرفتن دستگاه از پیمانکار در صورت وقوع شرایط عدم استفاده کاری از دستگاه طی یک سال	۱
۹	استفاده از سامانه‌های ردگیری و ردیابی برای اطلاع از موقعیت مکانی لحظه‌ای دستگاه	۱

جدول ۱۰- الزامات امنیت دستگاه‌های کاربران

ردیف	الزام	اولویت اقدام
۱	نصب و به‌روزرسانی مستمر وصله‌های امنیتی	۱
۲	استفاده از آنتی‌ویروس‌ها و آنتی‌باج‌افزارهای بروز شده با License معتبر	۱
۳	امن سازی سیستم‌عامل بر اساس چک‌لیست‌های CIS و STIG	۱
۴	حذف سرویس‌های غیرضروری همانند RDP[3]، Share و Power Shell	۱
۵	فعال‌سازی Firewall سیستم‌عامل	۱
۶	فعال‌سازی قفل خودکار صفحه‌نمایش	۱
۷	تنظیم گذرواژه برای BIOS	۱
۸	غیرفعال سازی اکانت‌های کاربری پیش‌فرض Guest و Administrator در سیستم‌عامل	۱

[1] Access Point Name
[2] Virtual Private Network
[3] Remote Desktop Protocol

- در راستای توسعه امن سامانه‌های مکانی، رعایت موارد مندرج در جدول ۱۱ و ۱۲ الزامی است. لازم به ذکر است که وجود گواهی ارزیابی امنیتی برای محصول (تأییدیه افتا)[1] که از سوی سازمان فناوری اطلاعات ایران صادر می‌گردد، به‌منزله رعایت موارد مذکور است. این موارد، گزیده‌ای از الزاماتی است که در سندهای راهنمای استاندارد همانند OWASP Web Security Testing Guide و OWASP Cheat Sheet Series آورده شده‌اند

جدول ۱۱- الزامات عمومی توسعه امن سامانه‌های مکانی

ردیف	الزام	اولویت اقدام
	حوزه تصدیق اصالت	
۱	فراهم کردن تصدیق اصالت[2] موجودیت‌ها[3] به کمک رهیافت‌های مبتنی بر نام کاربری و کلمه عبور و یا پروتکل‌هایی همانند OAuth[4]، OpenID، SAML[5] و FIDO[6] - در صورت استفاده از پروتکل OAuth باید از نسخه‌های OAuth 1.0a یا OAuth 2.0 بهره گرفته شود. - در صورت استفاده از پروتکل‌های OpenId یا SAML، سرویس‌دهنده IdP[7] باید در داخل سازمان مستقر شود.	۱
۲	استفاده از روش تصدیق اصالت چند فاکتوره (MFA[8]) برای عملکردهای حساس و پر ریسک سیستم و توجه به نکات زیر در استفاده از آن: - عدم ارسال اطلاعات محرمانه یا شخصی در کانال‌های جانبی همانند SMS و ایمیل - استفاده از توکن‌ها و پین‌های تصادفی - تعیین زمان اعتبار کوتاه برای توکن‌ها و پین‌ها	۱
۳	توجه به نکات زیر در پیاده‌سازی قابلیت تعریف نام‌های کاربری در سامانه: - عدم حساسیت شناسه‌ها و نام‌های کاربری به حروف کوچک و بزرگ - یکتا بودن شناسه‌ها - درصورتی‌که از آدرس ایمیل به‌عنوان شناسه کاربری استفاده شود، اعتبار آن باید بررسی شود.	۱
۴	عدم امکان تصدیق اصالت در سرورهای عمومی سامانه با استفاده از اکانت‌های مورداستفاده در سرورهای داخلی (به‌عنوان‌مثال راهبر سرور پایگاه‌داده‌ها نباید از اکانت خود در این سرور برای ورود به وب‌اپلیکیشن سامانه استفاده کند).	۱
۵	در نظر گرفتن پیچیدگی کافی در تدوین خط‌مشی تعریف کلمات عبور	۱
۶	پیاده‌سازی صحیح قابلیت بازیابی کلمه عبور و عدم امکان سوءاستفاده از آن	۱
۷	رمزنگاری کلمات عبور به کمک تکنیک‌های رمزنگاری غیرقابل‌بازگشت و قوی مانند الگوریتم درهم‌سازی Bcrypt	۱

[1] امنیت فضای تولید و تبادل اطلاعات

[2] Authentication

[3] موجودیت می‌تواند کاربر انسانی یا یک مولفه نرم‌افزاری باشد.

[4] Open Authentication
[5] Security Assertion Markup Language
[6] Fast Identity Online
[7] Identity Provider
[8] Multi Factor Authentication

ردیف	الزام	اولویت اقدام
۸	قفل‌کردن [1] اکانت کاربر پس از چندین تلاش ناموفق او برای تصدیق اصالت در سامانه و توجه به نکات زیر در پیاده‌سازی این قابلیت: - تعیین حداکثر تعداد دفعات تلاش‌های ناموفق برای تصدیق اصالت - تعیین حداکثر مدت‌زمان تلاش برای تصدیق اصالت - تعیین مدت‌زمان قفل ماندن اکانت	۱
۹	جلوگیری از افشای اطلاعات مهم طی پیام‌های خطایی که برای تصدیق اصالت ناموفق داده می‌شود	۱
۱۰	در صورت نیاز به نگهداری موقت اطلاعات کاربری سمت کلاینت باید از مکانیسم‌های امن برای ذخیره‌سازی آن‌ها استفاده شود.	۱
۱۱	اطمینان از تولید تصادفی CAPTCHA و استفاده از تکنیک‌هایی مانند چرخاندن، کشیدن و ایجاد موج در کاراکترها	۱
۱۲	استفاده از توکن مدت‌دار در صورت استفاده از روش‌های تصدیق اصالت مبتنی بر توکن در سرویس‌ها و تنظیم زمان موردنیاز تراکنش متناسب با فعالیت انجام‌شده	۱
	اعتبارسنجی ورودی‌ها	
۱۳	اعتبارسنجی تمام ورودی‌های سامانه برای جلوگیری از ورود داده‌های نادرست به جریان کاری سامانه و پایگاه داده‌ها و همچنین جلوگیری از حملات تزریق [2]. - قوانین اعتبارسنجی ورودی‌ها [3] باید بتوانند انواع ورودی‌های زیر را از نظر طول، مقدار و نوع، کنترل کنند: - فیلدهای ورودی فرم‌ها - فیلدهای مخفی - سرآیندهای HTTP - کوکی‌ها - URLها - دیگر مؤلفه‌های وبی	۱
	رویدادنگاری	
۱۴	ثبت و نگهداری اطلاعات رویدادهای سامانه به‌خصوص رویدادهای امنیتی [4]. نمونه‌ای از اطلاعاتی که باید ثبت شوند عبارت‌اند از: - نتیجه فرآیند تصدیق اصالت و مجازشماری موجودیت‌ها (شکست یا موفقیت) - شکست فرآیند اعتبارسنجی ورودی‌ها - شکست فرآیند مدیریت نشست - خطاهای زمان اجرای اپلیکیشن - مشکلات ارتباطی - مشکلات مربوط به کارایی - پیام‌های خطای مربوط به سرویس‌های جانبی - خطاهای مربوط به سیستم فایل‌ها	۱

[1] Lockout
[2] Injection
[3] Input Validation
[4] Logging

ردیف	الزام	اولویت اقدام
	- تشخیص ویروس در فایل‌های آپلود شده - تغییرات در پیکربندی - استفاده از عملکردهای حساس همانند برقراری ارتباطات شبکه‌ای، حذف و اضافه کاربران، تغییر در سطوح و مجوزهای دسترسی، اعطا و سلب توکن‌های دسترسی به کاربران و استفاده از مجوزهای راهبر نمونه‌ای از فیلدهای اطلاعاتی که باید برای هر رویداد نگهداری شوند عبارتند از: - تاریخ و زمان سیستم - تاریخ و زمان ثانویه (GPS) - نام کاربر یا موجودیتی که عمل مربوط به رویداد را انجام داده است - اطلاعات عمل مربوط به رویداد - اطلاعات کلاینت اعم از آدرس IP و پورت مبدا	
۱۵	جلوگیری از دسترسی غیرمجاز و سوءاستفاده از لاگ‌ها هنگام ذخیره‌سازی و انتقال	۱
۱۶	استفاده از رسانه‌های Read-Only برای نگهداری لاگ‌ها و حصول اطمینان از آن‌که عمل ثبت لاگ منجر به از دست رفتن منابع ذخیره‌سازی سیستم و ایجاد اختلال در عملکرد سایر سرویس‌ها نمی‌شود.	۱
۱۷	عدم ثبت داده‌های حساس همانند رمزهای عبور، توکن‌های دسترسی، کلیدهای رمزنگاری و غیره در لاگ‌ها	۱
۱۸	استفاده از فرآیندهای منظم برای نظارت بر رویدادها و ارائه گزارش‌ها و هشدارها بر مبنای این داده‌ها	۱
	مدیریت نشست	
۱۹	پیاده‌سازی فرآیند مدیریت نشست[1] برای نگهداری وضعیت موجودیت در حال تعامل با سامانه	۱
۲۰	در نظر گرفتن یک شناسه یا توکن به ازای هر نشست	۱
۲۱	استفاده از شناسه‌هایی با طول بیشتر از ۱۲۸ بیت برای نشست و هش کردن آن به کمک توابع مناسب	۱
۲۲	تغییر عناوین پیش‌فرضی که Frameworkهای مختلف برای شناسه نشست‌ها در نظر می‌گیرند (مثلاً در اپلیکیشن‌های مبتنی بر PHP عنوان پیش‌فرض این شناسه PHPSESSID نام دارد)	۲
۲۳	تنظیم زمان انقضا برای تمام نشست‌ها	۱
۲۴	عدم قرار دادن توکن یا شناسه نشست در URL	۱
۲۵	فراهم بودن مکانیسم‌های اتمام نشست	۱
۲۶	هشدار فعال شدن نشست کاربر در مکانی دیگر	۱
	کنترل خطا	
۲۷	کنترل انواع خطاها و استثناها[2] اعم از: - خطاهای پیش‌بینی‌شده - خطاهای پیش‌بینی‌نشده (مثلاً برای کنترل این خطاها می‌توان از یک صفحه خطای عمومی برای نمایش به کاربر استفاده کرد) - خطاهای فنی (خطاهای مربوط به زبان برنامه‌نویسی و چارچوب مورداستفاده مانند خطاهای مربوط به اندازه آرایه، حافظه و غیره)	۱

[1] Session Management
[2] Error/Exception Handling

ردیف	الزام	اولویت اقدام
	- خطاهای مربوط به منطق اپلیکیشن - خطاهای خاصی که نه فنی هستند و نه منطقی (مانند هنگامی‌که کاربر تصدیق اصالت شده بخواهد به ویژگی‌های غیرمجازی دسترسی یابد، خطایی ایجاد خواهد شد که باید به‌درستی کنترل شود)	
۲۸	اطمینان از عدم وجود اطلاعات بااهمیت در پیام‌های مربوط به خطاها و استثناها	۱
۲۹	ثبت خطاها در لاگ (زیرا ممکن است نشان‌دهنده یک مشکل در منطق اپلیکیشن یا بیانگر یک حمله باشند)	۱
	کنترل دسترسی	
۳۰	استفاده از ترکیب مدل‌های دسترسی RBAC[1] و ABAC[2] و در نظر گرفتن موارد زیر برای پیاده‌سازی مکانیسم کنترل دسترسی به داده‌های مکانی: - ویژگی‌های مکانی شیء موردنظر (همانند نوع پوشش جغرافیایی ناحیه مربوطه) - محتوای موضوعی ناحیه موردنظر - سطوح قابل بزرگنمایی - محل قرارگیری کاربر درخواست‌کننده - زمان ثبت داده‌ها یا زمان دسترسی کاربر درخواست‌کننده به داده‌ها	۲
	حفظ محرمانگی و صحت	
۳۱	رمزنگاری داده‌های حساس هنگام انتقال و ذخیره‌سازی - برخی از نکاتی که در انتخاب الگوریتم‌های رمزنگاری باید موردتوجه قرار گیرد: ○ طول کلید ○ کارایی و سرعت الگوریتم در انجام رمزنگاری و رمزگشایی ○ آسیب‌پذیری‌های الگوریتم در کتابخانه‌های مربوطه - برخی از نکاتی که در مورد کلیدهای رمزنگاری باید موردتوجه قرار گیرد: ○ تولید تصادفی کلیدها با استفاده از توابع امن زبان‌ها و Frameworkهای برنامه‌نویسی ○ در نظر گرفتن مدت‌زمان محدود برای دوره حیات کلیدها و تولید مجدد آن‌ها پس از انقضای این زمان ○ عدم ذخیره‌سازی کلیدها به‌صورت Hardcode شده در Source Code نرم‌افزار	۱
۳۲	حفاظت از فایل‌های پیکربندی حاوی کلید با در نظر گرفتن مجوزهای دسترسی محدود	۱
۳۳	محافظت از کلیدهای رمزنگاری به کمک روش‌هایی همانند رمزنگاری خود کلیدها	۲
۳۴	نگهداری کلیدها و داده‌ها در سیستم‌های مجزا و استفاده از مکانیسم‌های ذخیره‌سازی امن فراهم‌شده توسط سیستم‌عامل و Frameworkها برای کلیدها	۲
۲۵	فراهم کردن امکان تصدیق اصالت منبع داده‌ها و بررسی صحت آنها با تولید و وارسی امضاهایی از نوع متقارن (کد تصدیق اصالت پیام (MAC[3])) و غیرمتقارن (امضای دیجیتال) نوع غیرمتقارن، علاوه بر فراهم کردن امکان بررسی صحت و اصالت داده‌ها، قابلیت عدم انکار را نیز فراهم می‌کند.	۳

[1] Rule-Based Access Control
[2] Attribute-Based Access Control
[3] Message Authentication Code

وزارت نیرو
کارگروه تخصصی
امنیت سایبری

جدول ۱۲- الزامات اختصاصی توسعه امن سامانه‌های مکانی همراه

ردیف	الزام	اولویت اقدام
۱	اعمال محدودیت در نصب نرم‌افزار از طریق ثبت کد IMEI[1] دستگاه‌های مجاز	۱
۲	اعمال تاریخ اعتبار روی نرم‌افزار نصب‌شده بر روی دستگاه	۱
۳	استفاده از سرویس‌های اختصاصی مانند APN (که توسط اپراتورهای داخل کشور پشتیبانی می‌شوند) جهت تبادل اطلاعات با سرور	۱
۴	غیرفعال‌سازی امکان ارسال و دریافت در حالت بسته‌شده سیستم‌عامل دستگاه	۱
۵	رمزنگاری داده‌های ذخیره‌شده روی دستگاه	۱
۶	فراهم بودن قابلیت Block کردن IP های غیرمجاز	۱
۷	غیرفعال شدن نرم‌افزار در صورت عدم استفاده از دستگاه طی مدت مشخص (حداکثر پس از ۶ ماه با توجه به حساسیت کاربرد)	۱
۸	استفاده از روش‌های مبتنی بر توکن همانند استاندارد FIDO (UAF[2]) به همراه پارامترهای بیومتریک برای تصدیق اصالت کاربران دستگاه‌ها	۲

۴-۳-۵- توزیع و به اشتراک‌گذاری داده‌های مکانی

- در راستای تبادل امن داده از طریق سرویس‌های مکانی، رعایت موارد مندرج در جدول ۱۳ الزامی است.

جدول ۱۳- الزامات اختصاصی توسعه امن وب‌سرویس‌ها

ردیف	الزام	اولویت اقدام
	الزامات عمومی	
۱	استفاده از توکن مدت‌دار در صورت استفاده از روش‌های تصدیق اصالت مبتنی بر توکن در سرویس‌های مکانی و تنظیم زمان موردنیاز تراکنش متناسب با فعالیت انجام‌شده	۱
۲	استفاده از وب‌سرویس‌های رمزنگاری‌شده برای تبادل داده با سرور، در صورت ارسال آنلاین اطلاعات	۱
۳	تعریف و اعمال سطوح دسترسی برای سرویس‌های مکانی مطابق با جدول ۴	۱
۴	محدود کردن تعداد فراخوانی وب‌سرویس‌ها در یک بازه زمانی مشخص	۱
۵	استفاده از Parser های امن برای اعتبارسنجی ساختار پیام‌ها برای جلوگیری از حملاتی همانند XML DoS	۱
۶	محدود کردن اندازه پیام‌های مبادله شده با وب‌سرویس‌ها	۱
۷	استفاده از بسترهای امن همانند HTTPS برای دسترسی به وب‌سرویس‌ها	۱
۸	در پیاده‌سازی سرویس‌های REST ful[3] موارد زیر باید رعایت گردد: - محدود کردن متدهای HTTP قابل استفاده	۱

[1] International Mobile Equipment Identity
[2] Universal Authentication Framework
[3] REpresentational State Transfer

وزارت نیرو
کارگروه تخصصی
امنیت سایبری

	- اعتبارسنجی نوع محتوای درخواست و پاسخ، با توجه به فیلدهای مربوطه در سرآیند HTTP - عدم قرار دادن اطلاعات حساس همانند API Key[1] و توکن‌های دسترسی، در URL - غیرفعال کردن قابلیت CORS[2] در صورت عدم نیاز به آن	
الزامات سرویس‌های OGC		
۹	با توجه به دسترسی مستقیم به پایگاه داده در سرویس‌های دارای Data Access مانند WFS و Feature Server، استفاده از آن‌ها در نرم‌افزارهای تحت وب تا حد امکان محدود شده و ترجیحاً در نرم‌افزارهای دسکتاپ ایجاد گردند.	۱
۱۰	در صورت استفاده از سرویس WPS، از عدم امکان واکشی و ارسال اطلاعات در سایر مسیرها مانند Email و غیره اطمینان حاصل گردد.	۱

- در راستای ایجاد کانال‌ها و مسیرهای امن و مورد اعتماد برای به اشتراک‌گذاری و انتقال داده‌ها، رعایت موارد مندرج در جدول ۱۴ الزامی است.

جدول ١٤- الزامات امنیتی مسیرهای اشتراک‌گذاری و انتقال داده‌های مکانی

ردیف	الزام	اولویت اقدام
۱	محدودسازی تبادل داده و اطلاعات مکانی از طریق ذخیره بر روی ذخیره‌سازها مانند CD-DVD، Hard یا Flash، و در اولویت قراردادن تبادل داده به‌صورت سیستمی	۱
۲	امن‌سازی کلیه‌ی تجهیزات و سرویس‌های شبکه و زیرساخت (مانند سوئیچ، روتر، سرویس‌ها و پروتکل‌های مرتبط با آن) بر اساس چک‌لیست‌های موجود در سازمان و مبتنی بر مبانی همانند چک‌لیست‌های اختصاصی تولیدکنندگان محصولات مانند CISCO و چک‌لیست‌های CIS و STIG. به‌عنوان‌مثال تنظیم سرویس SSH[3] برای برقراری ارتباطات راه دور	۱
۳	استفاده از بسترها و تونل‌های امن همانند IPSec[4] و TLS[5] برای انتقال داده‌های مکانی بین مؤلفه‌های مختلف معماری و همچنین توزیع و به اشتراک‌گذاری داده‌ها	۱
۴	تغییر شناسه و رمز عبور پیش‌فرض تجهیزات شبکه	۱
۵	مسدودسازی IPهای ممنوع‌شده توسط مراجع ذیصلاح	۱
۶	نصب و پیکربندی انواع تجهیزات امنیتی همانند UTM[6] در شبکه و به‌روزرسانی آن‌ها متناسب با نیازمندی‌ها	۳
۷	استفاده از سامانه‌های ضد سرقت DLP[7] برای محافظت از سرورهای GIS	۳

[1] Application Programming Interface
[2] Cross Origin Resource Sharing
[3] Secure Shell
[4] IP Secure
[5] Transport Layer Security
[6] Unified Threat Management
[7] Data Loss Prevention

۵-۳-۵- حذف داده‌های مکانی

در راستای حذف امن داده‌های مکانی، اجرای موارد مندرج در جدول ۱۵ الزامی است.

جدول ۱۵- الزامات حذف امن داده‌های مکانی

ردیف	الزام	اولویت اقدام
۱	استفاده از روش‌های غیرقابل‌بازگشت برای حذف امن داده‌ها همانند: - بازنویسی رسانه ذخیره‌سازی با داده‌های جدید - غیرقابل استفاده کردن رسانه‌های ذخیره‌سازی - تخریب رسانه	۱
۲	استفاده از روش‌های Crypto-Shredding برای حذف داده‌های مکانی رمزنگاری‌شده‌ای که به‌عنوان داده‌های حساس شناخته می‌شوند.	۲

۶- بازنگری

این سند به‌صورت دوره‌ای یا در صورت بروز تغییراتی که بر آن تأثیرگذار هستند، به‌منظور تضمین تناسب با نیازمندی‌های امنیتی وزارت نیرو و شرکت‌های تابعه مورد بازبینی و تجدیدنظر قرار خواهد گرفت.

پیوست شماره ۱: گردآورندگان سند

تهیه مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	آزرم دهستانی منفرد	رئیس کارگروه فناوری اطلاعات مکانی وزارت نیرو	وزارت نیرو
برنامه‌ریزی و هماهنگی	مهنام فلاح	دبیر کارگروه فناوری اطلاعات مکانی وزارت نیرو	وزارت نیرو
تدوین و تنظیم	مهدیه قدسی نژاد	مشاور کارگروه فناوری اطلاعات مکانی وزارت نیرو	وزارت نیرو
تدوین و تنظیم	تینا تعویذی	مشاور کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت‌کننده	ناهید نیکپور	کارشناس سیستم های اطلاعات جغرافیایی دفتر فناوری اطلاعات، ارتباطات و آمار	شرکت توانیر
همکار مشارکت‌کننده	علی محرابی	کارشناس GIS دفتر فناوری اطلاعات و توسعه دولت الکترونیک	شرکت آب و فاضلاب کشور
همکار مشارکت‌کننده	محمد علی حائری	رئیس گروه سیستم های اطلاعاتی دفتر فناوری اطلاعات، توسعه مدیریت و تحول اداری	شرکت مدیریت منابع آب ایران
همکار مشارکت‌کننده	سید محسن بنی فاطمه	کارشناس ارشد سیستم اطلاعات مکانی دفتر هوشمندسازی و فناوری های نوین	شرکت توانیر
همکار مشارکت‌کننده	حمیدرضا خادم بروجردی	کارشناس تغییر اقلیم دفتر مطالعات اجتماعی، اقتصادی و زیست محیطی	سازمان انرژی‌های تجدیدپذیر و بهره‌وری انرژی برق (ساتبا)
همکار مشارکت‌کننده	امین حکیمی راد	کارشناس دفتر توسعه زیرساخت سیستم های اطلاعاتی و شبکه های ارتباطی	شرکت تولید نیروی برق حرارتی
همکار مشارکت‌کننده	رسول جلالی فر	مشاور کارگروه فناوری اطلاعات مکانی وزارت نیرو	وزارت نیرو
همکار مشارکت‌کننده	قاسم درخشان	مشاور کارگروه فناوری اطلاعات مکانی وزارت نیرو	شرکت اندیشه هوشمند مانا

بازنگری مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	دولت جمشیدی	رئیس کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
برنامه‌ریزی و هماهنگی	محسن کشاورز	دبیر کارگروه تخصصی امنیت سایبری	وزارت نیرو
همکار مشارکت‌کننده	سحر راکعی	عضو کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت‌کننده	تینا تعویذی	مشاور کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو

جمهوری اسلامی ایران
وزارت نیرو
کارگروه تخصصی
امنیت سایبری

تایید و تصویب مدرک

مسئولیت	نام و نام خانوادگی	عنوان	شرکت
راهبری	آزرم دهستانی متفرد	مدیر کل دفتر فناوری اطلاعات و آمار رئیس کارگروه تخصصی امنیت سایبری	وزارت نیرو
برنامه‌ریزی و هماهنگی	محسن کشاورز	دبیر کارگروه تخصصی امنیت سایبری	وزارت نیرو
همکار مشارکت‌کننده	امیره نیکخواه	مدیر کل دفتر فناوری اطلاعات، ارتباطات و آمار	شرکت توانیر
همکار مشارکت‌کننده	شهریار بهارلویی	مدیر کل دفتر فناوری اطلاعات و توسعه دولت الکترونیک	شرکت مهندسی آب و فاضلاب کشور
همکار مشارکت‌کننده	علی پرنیان	معاون دفتر فناوری اطلاعات، توسعه مدیریت و تحول اداری	شرکت مدیریت منابع آب
همکار مشارکت‌کننده	سید محسن ابطحی‌نژاد	مدیر کل دفتر فناوری اطلاعات، توسعه و زیر ساخت	شرکت تولید نیروی برق حرارتی
همکار مشارکت‌کننده	سید محسن زمزمیان	نماینده دفتر توسعه مدیریت و فناوری اطلاعات	سازمان انرژی‌های تجدیدپذیر و بهره‌وری انرژی برق (سانبا)
همکار مشارکت‌کننده	داود ابهت	مشاور فن آوری و هوشمندسازی	شرکت مدیریت ساخت و تهیه کالا آب و برق (ساتکاب)
همکار مشارکت‌کننده	دولت جمشیدی	سرپرست مرکز توسعه فناوری اطلاعات، ارتباطات و تجهیزات صنعت برق	پژوهشگاه نیرو
همکار مشارکت‌کننده	محمد خورشیدی	معاون حفاظت فناوری اطلاعات IT	وزارت نیرو
همکار مشارکت‌کننده	جلال جهانبخشی	نماینده دفتر مدیریت بحران و پدافند غیرعامل	وزارت نیرو

وزارت نیرو
کارگروه تخصصی
امنیت سایبری