



الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو
(Geospatial Information Technology Security Requirements)

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

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

تایید و تصویب	بازنگری	تهیه	
کارگروه تخصصی امنیت سایبری وزارت نیرو	کارگروه خدمات تخصصی امنیت سایبری	کارگروه فناوری اطلاعات مکانی وزارت نیرو	رکن نظام‌نامه
رئیس کارگروه	رئیس کارگروه	دبیر کارگروه	سمت
آزرم دهستانی منفرد	دولت جمشیدی	مهنم فلاح	نام
۱۴۰۰/۰۲/۱۸	۱۴۰۰/۰۲/۱۸	۱۴۰۰/۰۲/۱۸	تاریخ
			امضا



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	حلیقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری

جدول سوابق

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



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
وزارت نیرو	صفحه: ۲ از ۲۳		

فهرست مطالب

صفحه	عنوان
۳	۱- هدف و دامنه کاربرد.....
۳	۲- مراجع و اسناد مرتبط.....
۵	۳- تعاریف.....
۶	۴- مسئولیت.....
۷	۵- تشریح الزامات و روش اجرا.....
۷	۵-۱ ساختار اجرایی.....
۸	۵-۲ مدیریت کاربران و داده‌های مکانی.....
۱۰	۵-۳ الزامات چرخه حیات داده‌های مکانی.....
۱۰	۵-۳-۱ تولید، برداشت و جمع‌آوری داده‌های مکانی.....
۱۱	۵-۳-۲ ذخیره‌سازی داده‌های مکانی.....
۱۲	۵-۳-۳ پردازش و استفاده از داده‌های مکانی.....
۱۹	۵-۳-۴ توزیع و به اشتراک‌گذاری داده‌های مکانی.....
۲۱	۵-۳-۵ حذف داده‌های مکانی.....
۲۱	۶- بازنگری.....



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نسخه: ۱.۰	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نوع مدرک: روش اجرایی
	صفحه: ۳ از ۲۴	مرجع تصویب: کارگروه تخصصی امنیت سایبری	تاریخ: ۱۴۰۰/۰۲/۱۸ طبقه بندی: داخلی

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 مادر تخصصی، 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.



الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
 وزارت نیرو	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۴ از ۲۳

- Mohammad 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.



 وزارت نیرو	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	وزارت نیرو
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	
			صفحه: ۵ از ۲۳	

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^۱ محسوب می‌شود.

شیء مکانی: یک شیء قابل تشخیص که در یک محل مشخص با مختصات جغرافیایی منحصر به فرد قرار گرفته باشد، شیء مکانی^۲ نام دارد. دکل، پست برق، سد، تصفیه‌خانه، خط انتقال آب، رودخانه و غیره نمونه‌ای از این اشیاء هستند. هر شیء مکانی 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^۳ چارچوبی برای جمع‌آوری، ذخیره‌سازی، پازیبایی، 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^۴ 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.^۵

^۱ Geospatial Data
^۲ Spatial Object
^۳ Geospatial Information System
^۴ Spatial Data Infrastructure
^۵ jghg



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۶ از ۲۳

OGC Services: سازمان OGC^۱ استانداردهای موردنیاز برای دسترسی، نمایش و پردازش داده‌های مکانی را در قالب مجموعه‌ای از سرویس‌های وب تعریف کرده است که به آن‌ها OWS^۲ گفته می‌شود. WMS^۳، WFS^۴ و WCS^۵ نمونه‌ای از این سرویس‌ها هستند. درخواست‌های OWS به کمک پروتکل HTTP^۶ تعریف و به کمک ساختارهایی همانند XML^۷ کدگذاری می‌شوند.

چرخه حیات داده‌های مکانی: چرخه حیات داده‌های مکانی، توالی مراحل 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 مشخص شده 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.

^۱ Open Geospatial Consortium
^۲ OGC Web Service
^۳ Web Map Service
^۴ Web Feature Service
^۵ Web Coverage Service
^۶ Hypertext Transfer Protocol
^۷ Extensible Markup Language



الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
 وزارت نیرو	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	ملیقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۷ از ۲۳

۵- تشریح الزامات و روش اجرا

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

۱-۵- 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^۱ کلیه داده‌های مکانی مورد استفاده 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 مشخص شده در مفاد سند را که به‌عنوان اولویت اقدام ۱ تعیین شده‌اند، بر روی کلیه موارد شناسایی شده 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.



^۱ فراداده، نقشه‌ها، فایل‌های GIS و دیگر منابع داده‌ای مبتنی بر مکان را توصیف می‌کند.

	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	وزارت نیرو
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	

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 تأیید 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 اسناد به مفاد سند حاضر الزامی است.
- تبادل داده و اطلاعات مکانی در مجموعه وزارت نیرو (فی‌مابین هر سه سطح و بین شرکت‌های مادر تخصصی) با رعایت موارد مندرج در سند حاضر بلا مانع 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 تأیید 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.



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	
	تاریخ: ۱۴۰۰/۰۲/۱۸	حلقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	صفحه: ۹ از ۲۳

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، بزرگمایی 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 قابل تحلیل 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
۱	سازمانی	متناسب با حوزه کاری	متناسب با نقش	متناسب با نقش	متناسب با نقش و با اعمال محدودیت
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	-



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	صفحه: ۱۰ از ۲۳

۵-۳- الزامات چرخه حیات داده‌های مکانی

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

۵-۳-۱- 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 عهده دارند. همچنین موظف‌اند متناسب با روش برداشت مورد نظر، الزامات جدول ۴ را در پیوست قراردادهای برداشت و جمع‌آوری اطلاعات مکانی لحاظ کنند.

جدول ۴- الزامات امنیتی تولید، برداشت و جمع‌آوری داده‌های مکانی

ردیف	روشی و ابزار برداشت	الزام	اولویت اقدام
۱	دوربین‌های نقشه‌برداری، گیرنده‌های GNSS ^۱ (استاتیک و RTK ^۲)، سنجنده‌های مورد استفاده برای برداشت اطلاعات زیرسطحی مانند GPR ^۳ و غیره، دستگاه‌های مورد نیاز برای برداشت اطلاعات نقشه‌های هیدروگرافی مانند اکوساندر و غیره	در زمان تخلیه اطلاعات، چنانچه امکان ارسال اطلاعات جمع‌آوری شده 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 ۵-۳-۳ (برداشت و استفاده از داده‌های مکانی) در نرم‌افزار همراه مربوطه	۱
۳	پهپاد (UAV ^۴) و دوربین‌های عکاسی	- انعقاد قرارداد فقط با مشاوران دارای صلاحیت برداشت داده با پهپاد^۴ - اخذ مجوزهای رسمی لازم از مراجع ذیصلاح (نظامی/امنیتی) - نظارت نماینده GIS در زمان پرواز، تخلیه و پردازش اطلاعات	۱
۴	سنسورهای LiDAR ^۵	- با توجه به وجود افزونگی داده در داده‌های LiDAR لازم است: - فیلترگذاری‌های لازم بر روی داده خام اعمال شود تا فقط داده‌های مورد نیاز استخراج شده و در پایگاه داده ذخیره گردند. - داده‌ها می‌بایست صرفاً پس از پردازش و تولید عوارض مورد نیاز در قالب نقشه و با فرمت‌های معمول برداری، در اختیار کاربران قرار گیرد.	۱

^۱ Global Navigation Satellite System

^۲ Real-time kinematic positioning

^۳ Ground-penetrating radar

^۴ Unmanned Aerial Vehicle

^۵ صلاحیت مشاوران، توسط سازمان نقشه برداری کشور و براساس آیین نامه‌ها و دستورالعمل‌های آن سازمان تعیین و احراز می‌گردد.

^۶ Light Detection and Ranging



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	تاریخ: ۱۴۰۰/۰۲/۱۸
	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	صفحه: ۱۱ از ۲۳	

ردیف	روش و ابزار برداشت	الزام	اولویت اقدام
۱		نگهداری داده‌ها در فرمت‌های متعارف ابر نقطه ^۱ مانند las.	۱
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 ^۲ , STIG ^۳	۱
۲	استفاده از مکانیسم‌های حفاظتی مانند Firewall پایگاه داده‌ها و پراکسی معکوس برای حفاظت از درخواست‌های ارسالی به سرورهای پایگاه داده‌ها در برابر حملاتی همانند SQL Injection و جلوگیری از نشت اطلاعات در پاسخ‌های تولیدشده	۲
۳	مدیریت متمرکز کلیه دسترسی‌ها (مطابق جدول ۴) به پایگاه داده، توسط راهبر سیستم مدیریت پایگاه داده	۱
۴	رمزنگاری ^۴ داده‌های مکانی حساس موجود در پایگاه داده‌ها با استفاده از روش‌هایی همانند TDE ^۵ ، رمزنگاری قابل جستجو (SE) ^۶ و رمزنگاری لایه‌ای و یا استفاده از مکانیسم برچسب‌گذاری ^۷ داده‌ها و انواع رویکردها با سطوح مختلف ریزدانه‌گی مثلاً در سطح فیلد	۲

جدول ۶- 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 Administrator و Guest 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

^۱ 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.

^۲ Center for Internet Security

^۳ Security Technical Implementation Guide

^۴ Encryption

^۵ Transparent Data Encryption

^۶ Searchable Encryption

^۷ Labeling



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۳۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری

ردیف	الزام	اولویت اقدام
۴	فعال سازی آنتی ویروس ها و آنتی باج افزارهای بروز شده با License معتبر بر روی سرورهای GIS	۱
۵	ایجاد افزونگی ^۱ در انواع مؤلفه های زیرساخت ذخیره سازی و پردازش داده ها با بهره گیری از معماری چند ماشینی ^۲ در هر یک از سرورها، توزیع عملکرد سرور بین چند ماشین و استفاده از پراکسی معکوس ^۳ برای توازن بار بین سرورهای Back-end در GIS برای تأمین دسترسی پذیری بالا ^۴ (HA) به داده ها و مقابله با تهدید Single Point Of Failure با توجه به ریسک عدم تأمین سرویس (در این صورت سرور وب اپلیکیشن، درخواست های کلاینت را باید به این پراکسی ارسال کند).	۳
۶	مجزا کردن سرورهای (ماشین های مجازی) نقشه، وب اپلیکیشن و پایگاه داده ها از یکدیگر و رعایت این نکته که سرور پایگاه داده ها نباید در ناحیه DMZ ^۵ باشد.	۱
۷	استفاده از مکانیسم های حفاظتی مانند Firewall و وب اپلیکیشن (WAF ^۶) برای کنترل و آنالیز ترافیک پروتکل های HTTP و HTTPS که به وب اپلیکیشن وارد یا از آن خارج می شوند	۲
۸	تهیه و تحلیل مستمر گزارش های حوادث و خرابی های سرورهای GIS	۱

جدول ۷- الزامات آرشیو و پشتیبان گیری از داده های مکانی

ردیف	الزام	اولویت اقدام
۱	پیاده سازی خامشی تهیه نسخه های پشتیبان از داده ها (مطابق دستورالعمل مصوب کمیته تخصصی امنیت شرکت های مادر تخصصی) شامل تعداد نسخ پشتیبان و محل ذخیره سازی آن ها، روش پشتیبان گیری، نحوه دسترسی و همچنین مدت زمان نگهداری نسخه ها	۱
۲	استفاده از راهکارهای مدیریت دارایی های دیجیتال (DAM) ^۷ برای آرشیوها	۳
۳	استفاده از الگوریتم های رمزنگاری مورد تأیید سازمان برای حفاظت از آرشیوها	۳
۴	ذخیره و نگهداری نسخه های پشتیبان داده ها در محل های فیزیکی یا مجازی مستقل از محل ذخیره سازی داده های اصلی	۱
۵	انجام بررسی های لازم به صورت دستی یا به کمک مکانیسم هایی مانند Checksum پس از عملیات پشتیبان گیری، برای اطمینان از یکسان بودن تاریخ، اندازه و محتوای نسخه اصلی و پشتیبان	۳

۳-۵- پردازش و استفاده از داده های مکانی

- کلیه شرکت های تابعه موظف اند برای توسعه، پیاده سازی و استفاده از سامانه های مکانی به فهرست ابزارها و نرم افزارهای تجاری و نرم افزارهای متن باز که به تأیید کمیته امنیت وزارت نیرو رسیده است مراجعه کرده و

^۱ Redundancy
^۲ Multi-Machine Architecture
^۳ Reverse Proxy
^۴ High Availability
^۵ Demilitarized Zone
^۶ Web Application Firewall

^۷ پلتفرم ها و ابزارهای DAM (Digital Asset Management) امکان آرشیو انواع فایل ها اعم از مستندات متنی، تصاویر و غیره و همچنین مدیریت دسترسی به آنها را به صورت متمرکز فراهم می کنند.



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری صفحه: ۱۳ از ۲۳

استفاده از آن‌ها را در قراردادهای توسعه نرم‌افزار اعمال نمایند.^۱ ابزارها و موارد جدید پس از طرح در کمیته امنیت و اخذ تأیید 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 ^۲ آن	۱
۲	رعایت اصل اعطای حداقل مجوز موردنیاز ^۳ 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 ^۴ DoS و ^۵ DDoS در سطح اپلیکیشن و Proxy Page ^۶	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, Bing Maps, OSM ^۷ ، می‌بایست Tile‌های محدوده تحت پوشش شرکت داتلود و در سرور داخلی شرکت بارگذاری گردد تا به‌صورت آفلاین مورد استفاده قرار گیرند. - در دستگاه‌های همراه، قبل از شروع عملیات در محل، نقشه‌ها در حافظه دستگاه کش شده و به‌صورت آفلاین مورد استفاده 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

^۱ فهرست مذکور در پایگاه اینترنتی فناوری اطلاعات مکانی وزارت نیرو به آدرس <https://git.moe.gov.ir> در دسترس است.

^۲ Authorization

^۳ Least Privilege Principle

^۴ Denial of Service

^۵ Distributed Denial of Service

^۶ با توجه به ضرورت استفاده از دو Webserver جداگانه در سامانه‌های مکانی، به علت وجود Map server ها، استفاده از Proxy Page ضروری است.

^۷ Open Street Map



 وزارت نیرو	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۱۴ از ۲۳

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 ^۱ 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 ^۲ 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	تحويل گرفتن دستگاه از پیمانکار در صورت وقوع شرایط عدم استفاده کاری از دستگاه «لی یک سال	۱
۹	استفاده از سامانه‌های ره‌گیری 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 آنتی‌یافزارهای بروز شده با License معتبر	۱
۳	امن سازی سیستم‌عامل بر اساس چک‌لیست‌های CIS و STIG	۱
۴	حذف سرویس‌های غیرضروری همانند Power Shell و Share و RDP ^۳	۱
۵	فعال سازی Firewall سیستم‌عامل	۱
۶	فعال سازی قفل خودکار صفحه‌نمایش	۱
۷	تنظیم گذرواژه برای BIOS	۱
۸	غیرفعال سازی اکانت‌های کاربری پیش‌فرض Administrator و Guest در سیستم‌عامل	۱

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



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰	وزارت نیرو
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	

• 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)^۱ 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 ^۲ موجودیت‌ها ^۳ به کمک رهیافت‌های مبتنی بر نام کاربری و کلمه عبور و یا پروتکل‌هایی همانند ^۴ OAuth، OpenID، SAML ^۵ و FIDO ^۶ - 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 ^۷ IdP باید در داخل سازمان مستقر شود.	۱
۲	استفاده از روش تصدیق اصالت چند فاکتوره (MFA) ^۸ برای عملکردهای حساس و پر ریسک سیستم و توجه به نکات زیر در استفاده از آن: - عدم ارسال اطلاعات محرمانه یا شخصی در کانال‌های جایی 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 - پکتا بودن شناسه‌ها - در صورتی که 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 مورد استفاده در سرورهای داخلی (به‌عنوان مثال 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 خدماتی تعریف کلمات عبور	۱
۶	پیاده‌سازی صحیح قابلیت بازبینی کلمه عبور و عدم امکان سوءاستفاده از آن	۱
۷	رمزنگاری کلمات عبور به کمک تکنیک‌های رمزنگاری غیرقابل بازگشت و قوی مانند الگوریتم درهم‌سازی Bcrypt	۱

^۱ امنیت فضای تولید و تبادل اطلاعات^۲ Authentication^۳ موجودیت می‌تواند کاربر انسانی یا یک مولفه نرم‌افزاری باشد.^۴ Open Authentication^۵ Security Assertion Markup Language^۶ Fast Identity Online^۷ Identity Provider^۸ Multi Factor Authentication

الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۱۶ از ۲۳

ردیف	الزام	اولویت اقدام
۸	قفل کردن^۱ اکانت کاربر پس از چندین تلاش ناموفق او برای تصدیق اصالت در سامانه و توجه به نکات زیر در پیاده سازی این قابلیت: - تعیین حداکثر تعداد دفعات تلاش های ناموفق برای تصدیق اصالت - تعیین حداکثر مدت زمان تلاش برای تصدیق اصالت - تعیین مدت زمان قفل مائن اکانت	۱
۹	جلوگیری از افشای اطلاعات مهم طی پیام های خطایی که برای تصدیق اصالت ناموفق داده می شود	۱
۱۰	در صورت نیاز به نگهداری موقت اطلاعات کاربری سمت کلابنت باید از مکانیسم های امن برای ذخیره سازی آن ها استفاده شود.	۱
۱۱	اطمینان از تولید تصادفی CAPTCHA و استفاده از تکنیک هایی مانند چرخاندن، کشیدن و ایجاد موج در کاراکترها	۱
۱۲	استفاده از توکن مدت دار در صورت استفاده از روش های تصدیق اصالت مبتنی بر توکن در سرویس ها و تنظیم زمان مورد نیاز تراکنش متناسب با فعالیت انجام شده	۱
اعتبارسنجی ورودی ها		
۱۳	اعتبارسنجی تمام ورودی های سامانه برای جلوگیری از ورود داده های نادرست به جریان کاری سامانه و پایگاه داده ها و همچنین جلوگیری از حملات تزریق^۱: - قوانین اعتبارسنجی ورودی ها^۲ باید بتوانند انواع ورودی های زیر را از نظر طول، مقدار و نوع، کنترل کنند: - فیلدهای ورودی فرم ها - فیلدهای مخفی - سرآیندهای HTTP - کوکی ها - URL ها - دیگر مؤلفه های وبی	۱
رویدادننگاری		
۱۴	ثبت و نگهداری اطلاعات رویدادهای سامانه به خصوص رویدادهای امنیتی^۳، نمونه ای از اطلاعاتی که باید ثبت شوند عبارتند از: - نتیجه فرایند تصدیق اصالت و مجازسازی موجودیت ها (شکست یا موفقیت) - شکست فرایند اعتبارسنجی ورودی ها - شکست فرایند مدیریت نشست - خطاهای زمان اجرای اپلیکیشن - مشکلات ارتباطی - مشکلات مربوط به کارایی - پیام های خطای مربوط به سرویس های جانبی - خطاهای مربوط به سیستم فایل ها	۱

^۱ Lockout^۲ Injection^۳ Input Validation^۴ Logging

الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	دلیقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
			صفحه: ۱۷ از ۲۳

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 کلانیت اعم از آدرس IP و پورت مبدأ	
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 آن که 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 فرایندهای منظم برای نظارت بر رویدادها و ارائه گزارش‌ها و هشدارها بر مبنای این داده‌ها	۱
مدیریت نشست		
۱۹	پیاده‌سازی فرایند مدیریت نشست ^۱ 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 ابلیکشن‌های 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^۲ 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 مورد استفاده مانند خطاهای مربوط به اندازه آرایه، حافظه و غیره)	۱

^۱ Session Management
^۲ Error/Exception Handling



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو			
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISecurityReq-V1.0	نسخه: ۱.۰	
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری	صفحه: ۱۸ از ۲۳

ردیف	الزام	اولویت اقدام
	- خطاهای مربوط به منطق ایلکیشن - خطاهای خاصی که نه فنی هستند و نه منطقی (مانند هنگامی که کاربر تصدیق اصالت شده بخواهد به ویژگی‌های غیرمجاز دسترسی یابد، خطایی ایجاد خواهد شد که باید به درستی کنترل شود)	
۲۸	اطمینان از عدم وجود اطلاعات بااهمیت در پیام‌های مربوط به خطاها و استنهاها	۱
۲۹	ثبت خطاها در لاگ (زیرا ممکن است نشان دهنده یک مشکل در منطق ایلکیشن یا بیانگر یک حمله باشند)	۱
کنترل دسترسی		
۳۰	استفاده از ترکیب مدل‌های دسترسی RBAC^۱ و ABAC^۲ 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 درخواست کننده - زمان ثبت داده‌ها یا زمان دسترسی کاربر درخواست کننده به داده‌ها	۲
حفظ محرمانگی و صحت		
۳۱	رمزنگاری داده‌های حساس هنگام انتقال و ذخیره‌سازی - برخی از نکاتی که در انتخاب الگوریتم‌های رمزنگاری باید مورد توجه قرار گیرد: - طول کلید - کارایی و سرعت الگوریتم در انجام رمزنگاری و رمزگشایی - آسیب پذیری‌های الگوریتم در کتابخانه‌های مربوطه - برخی از نکاتی که در مورد کلیدهای رمزنگاری باید مورد توجه قرار گیرد: - تولید تصادفی کلیدها با استفاده از توابع امن زبان‌ها و Frameworkهای برنامه‌نویسی - در نظر گرفتن مدت زمان محدود برای دوره حیات کلیدها و تولید مجدد آن‌ها پس از انقضای این زمان - عدم ذخیره‌سازی کلیدها به صورت Hardcode شده در Source Code نرم افزار	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 فراهم شده توسط سیستم‌عامل و Frameworkها برای کلیدها	۲
۳۵	فراهم کردن امکان تصدیق اصالت منبع داده‌ها و بررسی صحت آنها با تولید و واریسی امضاهایی از نوع متقارن (کد تصدیق اصالت پیام (MAC)) 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



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: 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 ^۱ IMEI 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	فراموشی 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 ^۲) به همراه پارامترهای بیومتریک برای تصدیق اصالت کاربران دستگاه‌ها	۳

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 پست‌های امن همانند HTTPS برای دسترسی به وب‌سرویس‌ها	۱
۸	در پیاده‌سازی سرویس‌های RESTful ^۳ موارد زیر باید رعایت گردد: - محدود کردن متدهای HTTP قابل‌استفاده	۱

^۱ International Mobile Equipment Identity^۲ Universal Authentication Framework^۳ REpresentational State Transfer

	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری

- اعتبارسنجی نوع محتوای درخواست و پاسخ، با توجه به فیلدهای مربوطه در سرآیند HTTP - عدم قرار دادن اطلاعات حساس همانند ^۱ API Key و توکن های دسترسی، در URL - غیرفعال کردن قابلیت CORS ^۲ در صورت عدم نیاز به آن	
الزامات سرویس های OGC	
۹	با توجه به دسترسی مستقیم به پایگاه داده در سرویس های دارای Data Access مانند WFS و Feature Server، استفاده از آن ها در نرم افزارهای تحت وب تا حد امکان محدود شده و ترجیحاً در نرم افزارهای دسکتاپ ایجاد گردند.
۱۰	در صورت استفاده از سرویس WFS، از عدم امکان واکشی و ارسال اطلاعات در سایر مسیرها مانند Email و غیره اطمینان حاصل گردد.

- در راستای ایجاد کانال ها و مسیرهای امن و مورد اعتماد برای به اشتراک گذاری و انتقال داده ها، رعایت موارد مندرج در جدول ۱۴ الزامی است.

جدول ۱۴- الزامات امنیتی مسیرهای اشتراک گذاری و انتقال داده های مکانی

ردیف	الزام	اولویت اقدام
۱	محدودسازی تبادل داده و اطلاعات مکانی از طریق ذخیره بر روی ذخیره سازها مانند Hard، CD-DVD یا Flash، و در اولویت قراردادن تبادل داده به صورت سیستمی	۱
۲	امن سازی کلیه ی تجهیزات و سرویس های شبکه و زیرساخت (مانند سوئیچ، روتر، سرویس ها و پروتکل های مرتبط با آن) بر اساس چکلیست های موجود در سازمان و مبتنی بر منابعی همانند چکلیست های اختصاصی تولید کنندگان محصولات مانند CISCO و چکلیست های CIS و STIG به عنوان مثال تنظیم سرویس SSH ^۳ برای برقراری ارتباطات راه دور	۱
۳	استفاده از بسترها و تونل های امن همانند ^۴ IPSec و ^۵ TLS برای انتقال داده های مکانی بین مؤلفه های مختلف معماری و همچنین توزیع و به اشتراک گذاری داده ها	۱
۴	تغییر شناسه و رمز عبور پیش فرضی تجهیزات شبکه	۱
۵	مسدودسازی IP های ممنوع شده توسط مراجع ذیصلاح	۱
۶	نصب و پیکربندی انواع تجهیزات امنیتی همانند ^۶ UTM در شبکه و به روزرسانی آن ها متناسب با نیازمندی ها	۳
۷	استفاده از سامانه های ضد سرقت ^۷ DLP برای محافظت از سرورهای GIS	۳

^۱ Application Programming Interface

^۲ Cross Origin Resource Sharing

^۳ Secure Shell

^۴ IP Secure

^۵ Transport Layer Security

^۶ Unified Threat Management

^۷ Data Loss Prevention



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	حلیقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری
وزارت نیرو	صفحه: ۲۱ از ۲۳		

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 غیرقابل بازگشت 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 رمزنگاری شده‌ای که به‌عنوان داده‌های حساس شناخته می‌شوند.	۳

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.



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری

صفحه: ۲۲ از ۲۳

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
برنامه ریزی و هماهنگی	مهنم 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 تمویذی	مشاور کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت کننده	ناهید نیکپور	کارشناس سیستم های اطلاعات جغرافیایی دفتر فناوری اطلاعات، ارتباطات و آمار	شرکت توانیر
همکار مشارکت کننده	علی محرابی	کارشناس GIS دفتر فناوری اطلاعات و توسعه دولت الکترونیک	شرکت آب و فاضلاب کشور
همکار مشارکت کننده	محمد علی حائری	رئیس گروه سیستم های اطلاعاتی دفتر فناوری اطلاعات، توسعه مدیریت و تحول اداری	شرکت مدیریت منابع آب ایران
همکار مشارکت کننده	سید محسن بنی فاطمه	کارشناس ارشد سیستم اطلاعات مکانی دفتر هوشمندسازی و فناوری های نوین	شرکت توانیر
همکار مشارکت کننده	حمیدرضا خادم بروجردی	کارشناس تغییر اقلیم دفتر مطالعات اجتماعی، اقتصادی و زیست محیطی	سازمان انرژی های تجدیدپذیر و بهره وری انرژی برق (ساتبا)
همکار مشارکت کننده	امین حکیمی راد	کارشناس دفتر توسعه زیرساخت سیستم های اطلاعاتی و شبکه های ارتباطی	شرکت تولید نیروی برق حرارتی
همکار مشارکت کننده	رسول جلالی فر	مشاور کارگروه فناوری اطلاعات مکانی وزارت نیرو	وزارت نیرو
همکار مشارکت کننده	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
برنامه ریزی و هماهنگی	محسن کشاورز	دبیر کارگروه تخصصی امنیت سایبری	وزارت نیرو
همکار مشارکت کننده	سحر راکمی	عضو کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو
همکار مشارکت کننده	تینا تمویذی	مشاور کارگروه خدمات تخصصی امنیت سایبری	پژوهشگاه نیرو



	الزامات امنیتی فناوری اطلاعات مکانی وزارت نیرو		
	نوع مدرک: روش اجرایی	شناسه: ECS-MOE-G-PR-GISSecurityReq-V1.0	نسخه: ۱.۰
	تاریخ: ۱۴۰۰/۰۲/۱۸	طبقه بندی: داخلی	مرجع تصویب: کارگروه تخصصی امنیت سایبری

تایید و تصویب مدرک

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

