وزارت مالیه
جمهوری اسلامی افغانستان

وزارت مخابرات و تکنالوجی معلوماتی
جمهوری اسلامی افغانستان

بانک انکشاف آسیایی

پالیسی دسته بندی

اطلاعات جغرافیایی (مکانی) افغانستان

ایجاد انعطاف پذیری در برابر شکنندگی در پروژه های تحت پشتیبانی بانک انکشاف آسیایی- سیستم اطلاعات جغرافیایی و خدمات تکنالوجی معلوماتی

بانک انکشاف آسیایی

نسخهٔ 1،0- سپتمبر 2017

شمارهٔ مرجع قرارداد: 122883-S52802

Alcis Holdings Ltd.

فهرست عناوین

خلاصهٔ اجرایی

این سند پالیسی بیانگر آنست که حکومت افغانستان باید چگونه اطلاعات جغرافیایی (مکانی) و دارایی های اطلاعاتی خود را دسته بندی نماید تا از استفاده و نگهداری مناسب این اطلاعات اطمینان بعمل آورد؛ از کار سکتور عامه و بهره برداری موثر از اطلاعات پشتیبانی نماید و الزامات قوانین مربوطه و تعهدات و مکلفیت های بین المللی یا دو جانبه را برآورده نماید. این پالیسی در مورد تمام اطلاعات جغرافیایی (مکانی) که دولت در راستای عرضهٔ خدمات و انجام تجارت جمع آوری، ذخیره، تهیه، تولید یا منتشر می کند، تطبیق می گردد، از جمله اطلاعاتی که از همکاران خارجی دریافت و یا با آنها مبادله شده اند.

تمام ادارات حکومتی افغانستان و کارمندان آنها مکلف هستند تا محرمیت و انسجام هر گونه اطلاعات جغرافیایی (مکانی) حکومت و اطلاعاتی که بدان دسترسی دارند را حفظ نمایند و شخصاً موظف هستند تا بنا به هدایت این پالیسی از دارایی های اطلاعاتی حفاظت و حراست نمایند.

این پالیسی چهار اصل کلیدی برای تأمین، مدیریت و تشریک کارآمد اطلاعات جغرافیایی و معلومات مربوطه را تشریح می نماید که عبارتند از:

- **تمام** اطلاعات جغرافیایی و معلومات مربوطه دارای ارزش محوری بوده و نیاز به درجهٔ مناسبی از محافظت دارند؛
- **هر کسی** که با حکومت کار می کند، موظف به حفظ محرمیت و محافظت از اطلاعات جغرافیایی (مکانی) و معلومات مربوطه می باشد.
- دسترسی به اطلاعات **حساس** باید **صرفاً** همراه با تأمین تدابیر مقتضی برای کنترول امنیت پرسونل اعطا گردد؛ و
- اطلاعات دریافت شده یا مبادله شده با همکاران خارجی **باید** با همان درجهٔ محرمانگی حفظ شوند.

اطلاعات جغرافیایی (مکانی) و دارایی های اطلاعاتی مربوطه در یکی از سه کتگوری ذیل قرار می گیرند؛ عامه، برای استفاده داخلی یا محرمانه. هر یک از این کتگوری ها مجموعه ای از تدابیر امنیتی مبنایی را به خود اختصاص می دهند و به شکل مقتضی در برابر تهدیدات موجود حفاظت می شوند. افزون بر آن، ممکن است سیستم ها و خدمات تکنالوجی معلوماتی و ارتباطی نیازمند کنترول بهتر باشند تا خطرات موجود برای اطلاعات کلی (aggregated data) و یا نگرانی هایی که در مورد یکپارچگی و موجودیت اطلاعات وجود دارند، مدیریت شوند.

تمام ریاست ها و ادارات حکومت افغانستان می بایست این پالیسی را تطبیق نموده و از اجرای مداوم تدابیر کنترولی توسط تمام همکارانشان اطمینان بعمل آورند.

دسته بندی های امنیتی اطلاعات جغرافیایی (مکانی) حکومت افغانستان در تاریخ ششم سپتمبر 2017 انفاذ خواهند یافت.

دفتر مقام ریاست جمهوری

رفیع الدین ملک زی

مشاور ارشد مقام ریاست جمهوری

تعریفات

دیتا- به معنای جلوه ای از اطلاعات، مجموعه ها و مشاهدات عددی، اسناد، وقایع، نقشه ها، تصاویر، چارت ها، جداول، ارقام و مفاهیم می باشد که به اشکال دیجیتل یا انالوگ موجود می باشند.

اطلاعات جغرافیایی (مکانی)- تمام اطلاعاتی که دارای مرجع جغرافیایی می باشند.

اطلاعات- معلومات تهیه شده.

اطلاعات کلان – عبارت از اطلاعاتی است که منبع، زمان، مکان و شرایط تولید آن، ذکر شده است. اطلاعات کلان به استفاده کنندگان اطلاع می دهند که چه کسی، چه اطلاعاتی را، چه وقت، در کجا، چرا و چگونه تولید نموده است. استفاده از اطلاعات کلان این امکان را به استفاده کنندگان می دهد تا اطلاعات مورد نظر را برای پیدا کردن یک منبع مشهور ردیابی کنند و به سطح کیفیت و اعتبار آن پی ببرند.

مالک اطلاعات- فرد یا گروهی از افراد است که به طور رسمی در قبال انتقال و استفادهٔ اطلاعات مشخص و ذخیرهٔ آن در یک یا چند سیستم یک نهاد مسئول پنداشته می شود.

سرپرست اطلاعات- کارمندی که دارای مسئولیت اداری یا عملیاتی در قبال اطلاعات نهاد می باشد.

مسئول اطلاعات- شخصی است که مسئولیت مدیریت و صحت عناصر اطلاعاتی_هم محتوا و اطلاعات کلان_ را بعهده دارد. کارکرد تخصصی مسئولین اطلاعات معطوف به پروسه ها، پالیسی ها، رهنمود ها و مدیریت تمام اطلاعات در مطابقت با مکلفیت های پالیسی و تنظیمی می باشد.

یکپارچگی یا انسجام اطلاعات: به طور عمومی اشاره به کامل بودن، دقت و سازگاری اطلاعات دارد.

دسترسی پذیری اطلاعات- اصطلاحی است برای توصیف محصولات و خدماتی که اطلاعات را در صورت لزوم در اختیار استفاده کنندگان نهایی قرار می دهند. این اصطلاح برای بیان این نکته بکار می رود که درجهٔ دسترسی پذیری فوری به اطلاعات چقدر است یا اینکه تا چه حد امکان مدیریت و تأمین دائمی اطلاعات وجود دارد.

مدیریت اطلاعات – اشاره به روندی دارد که در آن اطلاعات به طور ایمن در طول پروژه یا بعد از ختم آن، ذخیره، آرشیو و به جای دیگر انتقال داده می شوند. این روند مشتمل بر تدوین پالیسی ها و طرزالعمل های لازم برای مدیریت اطلاعات به روش الکترونیکی و به اشکال غیرالکترونیکی می باشد.

اطلاعات حساس- عبارت از اطلاعاتی است که باید در برابر دسترسی غیرمجاز حفظ شوند تا محرمیت یا امنیت شخص یا سازمان محفوظ باقی بماند. از بین رفتن، سوء استفاده، تعدیل یا دسترسی غیرمجاز به اطلاعات حساس می تواند تأثیر منفی بر محرمیت یا بهروزی یک سازمان یا شخص وارد کند و درجهٔ این تأثیرگذاری وابسته به میزان حساسیت و ماهیت اطلاعات می باشد.

اطلاعات محرمانه- عبارت از اطلاعاتی است که صرفاً بواسطهٔ پروسهٔ از قبل مقرر شدهٔ ثبت نام و تجویز توسط ریاست ها یا سازمان های ذیربط، قابل دسترسی می باشد.

متابعت

تمام نهادهای حکومت افغانستان مکلف هستند تا از الزامات قانونی، حقوقی و قراردادی مربوطه متابعت نمایند. پالیسی دسته بندی اطلاعات جغرافیایی (مکانی) بخشی از مجموعه پالیسی های امنیت اطلاعات می باشد که در صدد حصول اطمینان از این نکته است که اطلاعات تحت مالکیت ادارات حکومتی (از تولید گرفته تا نگهداری و یا تخریب) با حداکثر امنیت جهت برآورده کردن الزامات تجاری و الزامات متابعتی مربوطه مدیریت می شوند.

تخطی از احکام این پالیسی می تواند امتیاز استفاده از سیستم های اطلاعاتی نهاد را از متخلف صلب و یا به تعلیق در آورد. بنا به مجازات های اداری دیگری که وجود دارد، ممکن است اقدامات جزایی تا ختم دورهٔ اشتغال برای فرد متخطی تطبیق گردد و از طرف دیگر ممکن است اقدامات جبرانی مدنی، جزایی و معادل آن برای فرد متخطی در نظر گرفته شود.

صلاحیت

ارگ ریاست جمهوری افغانستان مالک این پالیسی می باشد و روند تدوین این پالیسی را از نزدیک نظارت نموده است. ارگ ریاست جمهوری با پشتیبانی مقام ریاست جمهوری این پالیسی را جهت استفاده در تمام ادارات حکومتی توشیح نموده است.

تاریخ بررسی پالیسی

نسخه	توصیف	تاریخ بازنگری	مولف
1.0	پالیسی توشیح شده	2017/09/06	السیس
1.1	(هر تغییری)		

پالیسی

1. هدف

هدف این پالیسی ایجاد چارچوبی است که با استفاده از آن اطلاعات جغرافیایی (مکانی) با توجه به میزان حساسیت، محرمیت و اهمیت آن برای حکومت و مردم افغانستان، دسته بندی شوند. دسته بندی اطلاعات به ما کمک می کند تا حداقل تدابیر امنیتی لازم را برای حفاظت از اطلاعات جغرافیایی (مکانی) و معلومات دیگر، کاربرد مناسب منابع و متابعت از قوانین وضع نماییم.

2. محدوده

2.1. این پالیسی در مورد تمام اطلاعات جغرافیایی (مکانی) و معلومات مربوطه ای که در اختیار ادارات دولتی افغانستان قرار دارند، تطبیق می شود. این پالیسی همچنان برای تمام کارمندان، همکاران و ادارات ثالث که اطلاعات جغرافیایی (مکانی) حکومت را در اختیار دارند، قابل اجرا می باشد.

2.2. این پالیسی اطلاعاتی را که توسط افراد برای اهداف شخصی استفاده شوند، تحت پوشش قرار نمی دهد.

3. پالیسی

تمام اعضای سیستم اطلاعات جغرافیایی که در نهادهای حکومت افغانستان حضور دارند، مکلف هستند تا از محرمیت، انسجام و اطلاعات تولید شده و در دسترس گذاشته شده، تعدیل یافته، منتشر شده، ذخیره شده یا استفاده شده توسط سازمان، بدون در نظرداشت نوعیت اطلاعات (برای مثال، الکترونیکی، کاغذی یا اشکال فزیکی دیگر) حفاظت نمایند.

با در نظر داشت این مسئولیت، واجب است که تمام اطلاعات سازمانی و سیستم هایی که با اطلاعات جغرافیایی (مکانی) سرو کار دارند، نظربه میزان حساسیتی که دارند، در یکی از کتگوری های سه گانهٔ ذیل قرار گیرند. این امر به تخصیص تدابیر امنیتی مقتضی برای تأمین کارایی اطلاعات کمک می کند و امکان متابعت از قوانین، مقررات، پالیسی ها، الزامات، استندردها و دیگر معیارهای مربوطه را فراهم می سازد. تمام مالکین، سرپرستان، استفاده کنندگان و مدیران اطلاعات مستقیماً مسئولیت دارند تا از ابلاغ بموقع فهرست های اطلاعات به استفاده کنندگان آن اطمینان حاصل نمایند.

هر یک از نهادهای حکومتی می بایست تمام اطلاعات جغرافیایی (مکانی) را شناسایی و بر مبنای درجهٔ اهمیت، محرمیت، حساسیت و دسترسی پذیری دسته بندی نماید. هر یک از نهادهای حکومتی باید از استفاده یا افشای اطلاعات به نحوی که به اصول دسته بندی این اطلاعات آسیب وارد نماید، جلوگیری نموده و در این راستا تدابیر مناسب را روی دست گیرند.

4. نگاه اجمالی به اصول کلیدی

4.1. این پالیسی به توصیف سیستم اداری حکومت افغانستان که برای تأمین، انتشار بموقع و مناسب اطلاعات جغرافیایی (مکانی) و معلومات مربوطه استفاده می شود، می پردازد.

اصل اول:
تمام اطلاعات جغرافیایی (مکانی) و معلومات مربوطه ای که باید توسط حکومت افغانستان و با هدف عرضهٔ خدمات و پیشبرد کار دولت، جمع آوری، ذخیره، تهیه، تولید یا منتشر شوند، دارای ارزش ذاتی بوده و مستلزم آن هستند که تحت درجهٔ مناسبی از حفاظت قرار گیرند.

4.2. در دسته بندی های امنیتی، حساسیت تمام اطلاعات جغرافیایی (مکانی) و معلومات مربوطه (در ابعاد تأثیر احتمالی ناشی از دسترسی غیرمجاز، از بین رفتن یا سوء استفاده) و لزوم حفاظت از آنها در برابر تهدیدات موجود نشان داده می شود. این دسته بندی در سه سطح صورت می گیرد:

4.3. این روش دسته بندی در مورد تمام اطلاعات جغرافیایی (مکانی) و دیگر معلومات مربوطه ای که توسط حکومت افغانستان جمع آوری، ذخیره، تهیه و تولید شده اند، تطبیق می شود. مجموعه های اطلاعات کلان و کلی ممکن است نیاز به کنترول جدی تری داشته باشند تا بدین طریق از خطرات وابسته به محرمیت، انسجام و دسترسی پذیری اطلاعات مدیریت جلوگیری به عمل آید.

4.4. ضروری است تا در هر یک از دسته های اطلاعات، مجموعه ای از تدابیر در زمینهٔ کنترول امنیت کارمندان، امنیت فزیکی و امنیت اطلاعات اتخاذ شود و این موارد تا حد مقتضی در برابر تهدیدات شناسایی شده حفاظت شوند. یک چارچوب کنترولی برای سطوح بالا به این پالیسی ضمیمه شده است (ضمیمهٔ 1). حداقل تدابیر کنترولی که باید عملی شود این است که تمام معلومات و اطلاعات جغرافیایی (مکانی) حکومت باید با احتیاط مدیریت شود تا الزامات قانونی و تنظیمی برآورده شود و خطر از بین رفتن و یا دسترسی نامناسب به اطلاعات کاهش یابد.

اصل دوم:
هر شخصی که با حکومت کار می کند (به شمول کارمندان، قراردادی ها و عرضه کنندگان خدمات) مکلف به حفظ محرمیت و حفاظت از اطلاعات جغرافیایی (مکانی) حکومت افغانستان و معلومات مربوطه ای است که بدان دسترسی دارد.

4.5. آسیب اتفاقی یا عمدی، دسترسی غیرمجاز، از بین بردن یا سوء استفاده از اطلاعات جغرافیایی (مکانی) و اطلاعات مربوطهٔ حکومت افغانستان به عنوان لطمه وارد کردن به اطلاعات در نظر گرفته می شود و می تواند تخلف جزایی پنداشته شود. افراد شخصاً مسئولیت دارند تا با دقت و احتیاط از این اطلاعات و معلومات مربوطه حفاظت کنند و در این راستا می بایست از رهنمایی لازم دربارهٔ الزامات امنیتی برخوردار شوند و تشریح شود که چه قوانینی ناظر بر نقش ها و مسئولیت های آنها می باشد، از جمله مجازات های احتمالی (تأدیبی یا جزایی) که می توانند در مورد رفتارهای ناشایست تطبیق شوند.

4.6. سازمان ها باید دارای یک سیستم مدیریت تخلفات باشند تا بتوانند به کشف و ابلاغ رفتارهای ناشایست کمک کنند، امکان تنفیذ طرزالعمل های تأدیبی را فراهم نمایند و از انجام تحقیقات جنایی پشتیبانی کنند.

اصل سوم:
دسترسی به معلومات و اطلاعات **حساس** باید **صرفاً** در صورت تشخیص "ضرورت واقعی برای دانستن به موضوع" و در صورت موجودیت تدابیر مقتضی برای تأمین امنیت پرسونل اعطاء شود.

4.7. اطلاعات باید در زمان مناسب به افراد مناسب سپرده شود. کوتاهی در تشریک یا بهره برداری از اطلاعات می تواند مانع پیشبرد موثر پروسه های تصمیم گیری حکومت شود و عواقب جدی به دنبال داشته باشد.

4.8. به طور عمومی، دسترسی غیرمجاز، از بین بردن یا سوء استفاده از اطلاعات حساس می تواند تأثیر قابل ملاحظه بر فرد، سازمان یا پیشبرد کار حکومت داشته باشد. دامنهٔ دسترسی به اطلاعات حساس باید به قدری باشد که برای اجرای کارآمد کار سازمان ضروری است و باید محدود به افرادی باشد که برای انجام یک کار بدان نیاز دارند و این دسترسی در شرایطی اعطاء شود که تدابیر کنترول امنیت پرسونل از قبل موجود باشد. اصل "نیاز به دانستن"[1] در هر جایی از حکومت که اطلاعات حساس را جمع آوری، ذخیره، تهیه یا تشریک می کنند و به هنگام ارتباط با سازمان های عامه و خصوصی خارجی و همکاران بین المللی تطبیق می گردد.

4.9. شاید ضروری باشد تا اطلاعات حساس در اختیار اشخاصی که اجازهٔ لازم را ندارند، قرار گیرد، برای مثال زمانی که نیاز به اقدام عاجل برای حفظ جان یک فرد یا جلوگیری از وقوع جرم جدی وجود داشته باشد. در چنین شرایطی، باید از رویکرد عقل متعارف استفاده شود_ اگر زمان اجازه داد، باید گزینه های بدیل را مد نظر قرار دهیم و اقدامات لازم را برای حفاظت از منبع اطلاعات اتخاذ نماییم. اگر تردیدی در مورد اعطای اجازهٔ دسترسی به اطلاعات حساس وجود داشته باشد، این مربوطه باید قبل از اقدام به چنین کاری با مدیران خود مشورت نمایند.

اصل چهارم:
اطلاعات دریافت شده یا مبادله شده با همکاران خارجی **باید** مطابق با هر یک از الزامات قانونی و تنظیمی، از جمله توافقنامه ها و تعهدات بین المللی، حفاظت شوند.

4.10. این پالیسی به طور یکسان در مورد اطلاعات جغرافیایی (مکانی) و معلومات مربوطهٔ دیگر (از جمله تصاویر ماهواره ای) که توسط دیگران به حکومت عرضه می شوند، از جمله حکومت های خارجی، سازمان های بین المللی، موسسات غیردولتی و اشخاص خصوصی، تطبیق می شود.

4.11. در مواردی که توافقات امنیتی متقابل با حکومت های خارجی یا سازمان های بین المللی و در مورد موضوعات مشخص وجود داشته باشد، همان میزان حفاظت از اطلاعات می بایست الزامی پنداشته شود و در مورد هر گونه اطلاعات جغرافیایی (مکانی) و معلومات مربوطه (از جمله تصاویر ماهواره ای) که دریافت می شوند، می بایست همان درجه از حفاظت که در مورد دارایی های اطلاعاتی حکومت افغانستان تطبیق می گردد، لحاظ شود.

[1]. حکومت و سازمان های دیگر از این اصطلاح برای اشاره به محرمانه کردن اطلاعاتی که بسیار حساس می باشند، استفاده می کنند.

5. تعریف دسته های اطلاعات

5.1. درجه 1-اطلاعات عامه

اطلاعاتی که افشای غیرمجاز، تغییر یا از بین بردن آن خطر اندک برای نهاد یا اعضای آن به دنبال دارد و یا هیچ خطری بوجود نمی آورد، می بایست با عنوان **درجه 1-عامه** دسته بندی شوند. هرچند حفظ محرمیت "اطلاعات عامه" مستلزم کنترول اندک بوده و یا نیاز به هیچ نوع نظارت و کنترول ندارد، اما جلوگیری از تعدیل و یا تخریب غیرمجاز این اطلاعات مستلزم آن است که درجه ای از کنترول تطبیق شود.

اطلاعات عامه به عنوان اطلاعات حساس در نظر گرفته نمی شود؛ بنابراین، اطلاعات عامه می تواند بدون کدام محدودیت در دسترس هر یک از متقاضیان قرار گرفته و یا منتشر شود. انسجام اطلاعات عامه می بایست حفظ شود، زیرا این امر متضمن اعتبار و صحت این اطلاعات خواهد بود. مالک مجاز اطلاعات باید در صورت امکان اجازۀ تکثیر یا کاپی برداری از اطلاعات را بدهد تا از حفظ صحت اطلاعات در طول زمان اطمینان بعمل آید. این اطلاعات به طور پیش فرض در دستۀ "اطلاعات عامه" قرار می گیرند، مگر اینکه الزامات انتقال به دسته های بالاتر را برآورده نمایند.

5.2. درجه 2-اطلاعات داخلی

اطلاعاتی که افشای غیرمجاز، تغییر یا از بین بردن آن خطر متوسط برای نهاد و اعضای آن بوجود بیاورد، با عنوان "**درجه 2-داخلی**" دسته بندی می شوند. کنترول امنیتی به درجۀ معقول می بایست در مورد اطلاعاتی که در این سطح قرار می گیرند، تطبیق گردد؛ از جمله اینکه: این اطلاعات نباید بدون اجازۀ مالک آن به دستگاه های دیگر کاپی و منتقل شود؛ باید یک مکانیزم برای کنترول این اطلاعات وجود داشته باشد تا دسترسی فزیکی به آن (برای مثال با اختصاص کلمه عبور یا پسورد) محدود شود؛ باید مکانیزم هایی برای اعطای دسترسی کنترول شده وجود داشته باشد؛ و اقداماتی همچون رمزگذاری اطلاعات روی دست گرفته شود.

تقاضای دسترسی به اطلاعات داخلی می بایست به مالک اطلاعات که در قبال اطلاعات مسئولیت دارد، تقدیم شود و اجازۀ دسترسی به آن توسط شخص وی صادر گردد (جزئیات بیشتر در مورد نقش ها و مسئولیت های تعریف شده، در بخش ششم ارائه شده است). دسترسی به اطلاعات داخلی می تواند به اعضای گروه ها در تناسب با درجه بندی شغل و مسئولیت های شان اعطا گردد (دسترسی "مطابق به مسئولیت"). همچنین این دسترسی می تواند محدود به بخش های مشخصی از سازمان مورد نظر باشد.

اطلاعات داخلی از درجۀ حساسیت متوسط برخوردار می باشند و غالباً برای کمک به تصمیم گیری مورد استفاده قرار می گیرند. بنابراین مهم است که دسترسی به این اطلاعات بطور بموقع تأمین شود و صحت آن محفوظ باقی بماند. عدم تأمین این اطلاعات در هنگام ضرورت، تأثیرات منفی و خطرات متوسط برای نهاد به دنبال خواهد داشت.

انواع اطلاعات نامبرده در ذیل می بایست در دستۀ "اطلاعات داخلی" قرار گیرند. این یک فهرست کامل نیست و در صورت تغییر در قوانین می تواند تعدیل یابد.

5.2.1. **اطلاعات مربوط به امنیت عامه**- اطلاعات مربوط به امنیت عامه مشتمل بر اطلاعاتی است که جزئیات پلان ها و ترتیبات امنیتی عامه و یا رسامی ها و نقشه های مفصل ساختمان های عامه و تأسیسات زیربنایی را احتوا می کنند.

5.2.2. **اسناد پرسونل کارمند**- اطلاعاتی که اسناد و جزئیات پرسونل کارمند از جمله نام، وظیفه، ریاست مربوطه و غیره را پوشش می دهند، باید با عنوان "اطلاعات داخلی" دسته بندی شوند. هر گونه گفتگو، افشا و یا انتشار غیرمجاز جزئیات محرمانۀ کارمندان، عمل غیرقانونی و سوء استفاده از مقام محسوب می شود.

5.3.درجه 3- اطلاعات محرمانه

اطلاعاتی که افشای غیرمجاز، تغییر یا تخریب آن درجۀ قابل توجهی از خطر را برای نهاد و کارمندان آن به دنبال دارد، از جمله تهدیدات امنیتی برای کشور و حتی خسارات جانی، باید با عنوان **درجه 3-محرمانه** دسته بندی شوند. در خصوص این اطلاعات، تدابیر کنترول امنیتی در بالاترین سطح می بایست تطبیق گردد. دسترسی به اطلاعات محرمانه باید از مرحلۀ ایجاد تا تخریب کنترول شود و تنها به اشخاص وابسته به سازمان هایی که برای انجام کارشان نیاز به دسترسی به این اطلاعات دارند، اعطاء گردد. درخواست دسترسی به اطلاعات محرمانه باید به طور فردی صورت گیرد و سپس توسط *مالک اطلاعات* که در قبال چنین اطلاعاتی مسئولیت دارد، تصدیق شود.

اطلاعات محرمانه دارای حساسیت بالایی می باشند و ممکن است حاوی نکاتی در مورد حریم خصوصی افراد باشند یا دسترسی به آن بنا به قوانین افغانستان منع شده باشد. افزون بر آن، در صورتیکه این اطلاعات اشتباه باشند، به شکل غیرمناسب افشا شوند یا در هنگام نیاز در دسترس گذاشته نشوند، تأثیرات منفی آن بر سازمان مربوطه معمولاً بسیار زیاد خواهد بود.

اطلاعات محرمانه مشتمل بر موارد ذیل است:

5.3.1. **اطلاعات شخصی و اطلاعات شخصی قابل شناسایی:** اطلاعاتی حاوی جزئیات شخصی، به شمول آدرس، شمارۀ تماس، شمارۀ ملک و جزئیات در مورد مالک، باید در دستۀ اطلاعات محرمانه قرار گیرند.

5.3.2. **تصاویر ماهواره ای دارای وضاحت بالا (high resolution):** یکی از خطراتی که طی سال های اخیر وجود داشته است، استفاده از این تصاویر توسط گروه های تروریستی برای شناسایی هدف حملات شان بوده است و از این رو این اطلاعات باید محرمانه تلقی شوند تا از بهره برداری از آن توسط چنین گروه های جلوگیری شود.

5.3.3. **نقشه های توپوگرافیک:** نقشه های توپوگرافیک دارای مقیاس کلان، جزئیات پستی ها و بلندی های زمین، مسیر ها و تأسیسات انتقال فاضلاب و دیگر ابعاد غیرطبیعی را نمایش می دهند. این اطلاعات می بایست برای حفظ امنیت ملت در برابر دشمن محرمانه باشند.

6. نقش ها و مسئولیت ها

تمام کارمندان سازمان ملزم هستند که از الزامات و معیارهای وضع شده در این پالیسی پیروی کنند و این قاعده الزاماً محدود به کارمندان بخش سیستم معلومات جغرافیایی نمی باشد.

نقش ها و مسئولیت های ذیل برای تطبیق این پالیسی وضع شده اند:

6.1. **مالک اطلاعات**- مالک اطلاعات عبارت از سازمانی است که از صلاحیت قانونی و عملیاتی در ارتباط با اطلاعات مشخص شده برخوردار می باشد. مالک اطلاعات موظف به ارزیابی درجهٔ حساسیت محتوای اطلاعات، دسته بندی اطلاعات و تعیین میزان ضروری حفاظت از اطلاعات می باشد. وزرا، معین های تخنیکی وزرا و مدیران تکنالجی اطلاعاتی از این صلاحیت برخوردار خواهند بود و گرفتن تصدیق آنها برای دسترسی یافتن به اطلاعات محرمانه الزامی می باشد.

6.2. مالکان اطلاعات مسئولند تا اطمینان حاصل کنند که اطلاعات جغرافیایی (مکانی) به شکل مقتضی دسته بندی می شوند و طرزالعمل های لازم برای ذخیره، دسترسی، انتشار و از بین بردن اطلاعات وجود دارد و وسایلی که برای ذخیره کردن این اطلاعات استفاده می شوند، از پالیسی های امنیت و حفاظت از اطلاعات پیروی می کنند. مالکان اطلاعات می بایست به شکل دوره ای سطوح دسته بندی که برای اطلاعات مشخص شده است را با دقت مرور نمایند و از مناسبت و ارزش این دسته بندی برای سازمان با در نظرداشت تغییرات در الزامات قانونی و تنظیمی و تغییرات در الزامات مربوط به استفاده و مدیریت اطلاعات اطمینان بعمل آورند.

6.3. مالکان اطلاعات باید تعدیلاتی را که سرپرستان و مسئولان اطلاعات برای سطوح دسته بندی پیشنهاد نموده اند، مرور و تصدیق نمایند.

6.4. **سرپرست اطلاعات**- مدیر دیتابیس، مادل ساز اطلاعات، افسر ارشد اطلاعات و مدیر تکنالجی معلوماتی سازمان به عنوان سرپرستان اطلاعات در نظر گرفته می شوند. سرپرستان اطلاعات در قبال محیط تخنیکی و ساختار دیتابیس و همچنین نگهداری، انتقال و ذخیره ایمن اطلاعات و تطبیق قواعد کاری مربوطه مسئول می باشند. سرپرستان اطلاعات مسئولیت دارند تا زیربنای مطمئنی برای پشتیبانی از اطلاعات تأمین کنند و از میان دیگر موارد به تأمین امنیت فزیکی، ساختن و بازیابی نسخه های پشتیبان (backup)، اعطای دسترسی به کاربران سیستم با اجازهٔ مسئولان اطلاعات یا نمایندگان آنها، اجرا و مدیریت تدابیر کنترول اطلاعات مبادرت ورزند.

6.5. **مسئول اطلاعات**- مسئول اطلاعات شخصی است که مسئولیت مدیریت و صحت اطلاعات_هم محتوا و هم اطلاعات کلان_ را بر عهده دارد. کارکرد تخصصی مسئولین اطلاعات معطوف به پروسه ها، پالیسی ها، رهنمودها و مدیریت تمام اطلاعات در مطابقت با الزامات پالیسی و تنظیمی می باشد. مسئول اطلاعات می تواند بخشی از مسئولیت های خویش را به سرپرست اطلاعات محول نماید.

6.6. کارکرد کارشناس سیستم اطلاعات جغرافیایی مشابه به مسئول اطلاعات است که مسئولیت مستقیم سطوح عملیاتی و مدیریت اطلاعات را بر عهده دارد. کارشناس سیستم اطلاعات جغرافیایی در قبال امور مربوط به دسترسی به اطلاعات و تطبیق پالیسی و همچنین نامگذاری صحیح اطلاعات مسئولیت دارد.

6.7. مسئول اطلاعات از موارد ذیل اطمینان حاصل می کند: مناسب بودن اطلاعات برای هدف مورد نظر؛ استفادهٔ منسجم از اطلاعات؛ مستندسازی تذکرات در مورد استفادهٔ صحیح از اطلاعات؛ مستند سازی منابعی که صلاحیت هر یک از بخش های اطلاعات کلان را بر عهده دارند؛ و جلوگیری از دسترسی یا تغییر غیرمجاز اطلاعات.

6.8. **بکاربرندهٔ اطلاعات**- کاربران اطلاعات عبارت از افرادی هستند که به عنوان بخشی از وظایف شان یا برای انجام نقش ها و مسئولیت هایشان، نیاز به دسترسی و استفاده از اطلاعات دارند. افرادی که از دسترسی به اطلاعات داخلی و محرمانه برخوردار می شوند، از اعتماد ویژه ای برخوردار بوده و مسئولند تا امنیت و انسجام اطلاعات را حفظ نمایند.

6.9. تمام افرادی که به اطلاعات دسترسی و یا آن را استفاده و مدیریت می کنند، مسئولند تا قواعد لازم در خصوص مدیریت هر یک از دسته های اطلاعات را رعایت کرده و در مواردی که نیاز به وضاحت بیشتر در مورد نحوهٔ مدیریت اطلاعات یک سازمان دارند، مشورت مسئولان و سرپرستان اطلاعات را جویا شوند. استفاده کنندگان قبل از آنکه شروع به کار با اطلاعات بالاتر از سطح عامه نمایند، می بایست از آموزش های لازم برای متابعت از این پالیسی برخوردار شوند.

6.10. تمام افرادی که به اطلاعات یک سازمان دسترسی دارند و یا آن را استفاده و مدیریت می کنند، مسئولند تا هر گونه تخلف از قواعد این پالیسی را به مدیران مربوطهٔ خویش ابلاغ نمایند.

ضمایم

ضمیمۀ 1- مادل تهدیدات و نتایج امنیتی

دسته بندی های امنیتی درجۀ حساسیت اطلاعات جغرافیایی (مکانی) حکومت افغانستان را بازتاب می دهند و نشان می دهند که کدام تدابیر کنترولی ویژه می بایست روی دست گرفته شود تا این اطلاعات در برابر تهدیدات احتمالی متعدد حفظ شوند. تدابیر امنیتی وقایوی می بایست به نتایج ذیل در هر یک از سطوح دسته بندی نایل آیند:

پروفایل تهدیدات	کنترول امنیتی		
اهداف امنیتی	عامه	داخلی	محرمانه
امنیت شخصی (دسترسی به اطلاعات)	• دسترسی توسط افراد مجاز برای دلایل کاری مشروع	• اطمینان از اینکه صرفاً افراد شناخته شده و مورد اعتماد به اطلاعات دسترسی دارند	• اطمینان بالا از اینکه دسترسی به اطلاعات بطور سخت گیرانه ای منحصر به افراد شناخته شده و قابل اعتماد است
امنیت فزیکی (مدیریت، کاربرد، ذخیره، انتقال و تخریب اطلاعات)	• اقدامات احتیاطی متناسب برای جلوگیری از وارد آمدن آسیب فرصت طلبانه یا اتفاقی به اطلاعات • کنترول دسترسی به اطلاعات حساس	• کشف و مقابله با وارد آمدن آسیب عمدی به اطلاعات از طریق تطبیق زور و حملۀ مخفیانه	• اقدامات جدی و مستحکم برای جلوگیری از وارد شدن آسیب به اطلاعات از طریق حملات پیوسته، پیچیده یا خشونت بار
امنیت اطلاعات (ذخیره، کاربرد، تهیه یا انتقال اطلاعات)	• پیشگیری از آسیب عمدی به اطلاعات از طریق حملات ماشینی یا فرصت طلبانه • اقدام به کشف آسیب های باالفعل و بالقوه و واکنش به آن	• کشف و مقابله با آسیب عمدی از طریق افراد کارکشته، مصمم و برخوردار از منابع کافی	• اقدامات سخت گیرانه برای جلوگیری از وارد شدن آسیب به اطلاعات از طریق حملات پیوسته توسط افراد کارکشته، مصمم و برخوردار از منابع کافی

ضمیمهٔ 2- تعیین دسته های اطلاعات

روش دسته بندی اطلاعات جغرافیایی (مکانی) که در این سند بکار رفته است، مبتنی بر بهترین شیوه های بین المللی و الزاماتی است که طی روند سروی افراد ذیدخل توسط ارگان های حکومت افغانستان بیان شده است.

اهداف امنیتی

هدف از امنیت اطلاعات همانا حفاظت از محرمیت، انسجام و دسترسی پذیری مجموعه های اطلاعات جغرافیایی (مکانی) می باشد.

با دسته بندی و مدیریت صحیح اطلاعات، می توانیم نشان دهیم که هر گونه آسیب به محرمیت، انسجام یا دسترسی پذیری اطلاعات تا چه حد بر حکومت تأثیرگذار است.

تعیین دسته بندی

در هنگام تعیین دسته بندی های اطلاعاتی می توانیم سطح اطلاعات را با مراجعه به فهرست تأثیرات و با استفاده از هدف امنیتی که برای حفظ محرمیت (در جدول بالا) تعریف شده است، تشخیص دهیم. با توجه به هدف امنیتی مربوط به محرمیت، **پایین** برابر به ***درجه1-عامه***، **متوسط** برابر به ***درجه 2-داخلی***، **بالا** برابر به ***درجه3-محرمانه*** می باشد.

اطلاعاتی که افشا، تغییر یا تخریب غیرمجاز آن می تواند خطر متوسط برای سازمان و اعضای آن در پی داشته باشد، با عنوان درجه***2-داخلی*** دسته بندی می شوند.

برای تشخیص اینکه آیا اطلاعات در درجه***3-محرمانه*** قرار می گیرند یا خیر، باید سنجیده شود که دسترسی غیرمجاز، از بین بردن یا افشای نادرست آن چقدر خطر برای سازمان و اعضایش در پی دارد، به شمول تهدیدات امنیتی برای کشور و صدمات جانی.

سرپرستان اطلاعات می توانند مجموعهٔ اطلاعاتی را که برای مثال از بعد تقسیم بندی اداری (ملی، ولایتی، ولسوالی و غیره) دارای هدف یا کارکرد مشترکی می باشند، در یک دستهٔ واحد قرار دهند.

با دسته بندی کلی اطلاعات (aggregate data classification) بالاترین درجهٔ تأثیرگذاری اطلاعات موجود در یک سیستم بدست می آید. برای مثال، اگر اطلاعات یک سیستم مشتمل بر اطلاعات دارای درجهٔ تأثیرگذاری پایین، اطلاعات تکمیلی دارای درجهٔ تأثیرگذاری پایین و اطلاعات تکمیلی دارای درجهٔ تأثیرگذاری بالا باشد، در آن صورت درجهٔ تأثیرگذاری کلی برای سیستم دارنده یا تهیه کنندهٔ تمام این اطلاعات بالا خواهد بود (زیرا "بالا" در میان مقادیر جزئی پایین، متوسط و بالا، از همه بیشتر است). درجهٔ تأثیرگذاری بالا به ***درجه3-اطلاعات محرمانه*** ترجمه می شود. برای مثال، جزئیات زمین های ثبت شده در ریاست املاک_دارای درجهٔ تأثیرگذاری پایین می باشد، اما اگر حاوی نام و شماره تماس مالک باشد، در آنصورت می بایست با عنوان ***درجه3-محرمانه*** دسته بندی شود، حتی اگر حدود زمین به عنوان اطلاعات ***عامه*** در نظر گرفته شوند.

به منظور دسته بندی اطلاعاتی که مشخصاً در این پالیسی دسته بندی نشده اند، سازمان ها می بایست تمام اطلاعات شان را از نقطهٔ نظر درجهٔ تأثیرگذاری تحلیل نمایند. این یک رویکرد چند مرحله ای می باشد.

مرحلهٔ اول- تحلیل درجهٔ تأثیرگذاری بر مبنای میزان الزامی شدهٔ محرمانگی، انسجام و دسترسی پذیری.

مرحلهٔ دوم- تعیین دسته بندی عمومی اطالعات برای مثال، عامه، داخلی یا محرمانه.

مرحلهٔ سوم- تعیین، تطبیق و آزمون تدابیر الزامی شده برای کنترول امنیت.

مرحلهٔ چهارم- نظارت مداوم از تدابیر کنترول امنیت.

جدول ذیل باید به عنوان مرجع برای تعیین درجهٔ تأثیرگذاری آسیب های وارده به محرمانگی، انسجام و دسترسی پذیری اطلاعات مورد استفاده قرار گیرد.

تأثیر بالقوه			
بالا	**متوسط**	**پایین**	**هدف امنیتی**
تأثیرات منفی که افشای غیرمجاز اطلاعات بر امنیت کشور، عملیات ها، دارایی ها و اعضای سازمان وارد می کند، می تواند شدید و فاجعه بار باشد.	افشای غیرمجاز اطلاعات می تواند تا حد متوسط بر عملیات ها، دارایی ها یا اعضای سازمان، تأثیر منفی وارد نماید.	افشای غیرمجاز اطلاعات می تواند به طور محدودی تأثیرات ناگوار بر عملیات ها، دارایی ها یا اعضای یک سازمان وارد نماید.	**محرمیت**- ایجاد و حفظ محدودیت های مجاز در مورد دسترسی پذیر کردن و افشای اطلاعات، از جمله بکارگیری وسایل لازم برای حفظ امنیت کشور، حراست از عملیات و وجههٔ سازمان، حراست از حریم شخصی و اطلاعات ملکیتی.
تأثیرات منفی که تعدیل یا تخریب غیرمجاز اطلاعات بر امنیت کشور، عملیات ها، دارایی ها یا اعضای سازمان وارد می کند، می تواند شدید و فاجعه بار باشد.	تعدیل یا تخریب غیرمجاز اطلاعات می تواند تا حد متوسط بر عملیات ها، دارایی ها و اعضای سازمان، تأثیر منفی وارد نماید.	تعدیل یا تخریب غیرمجاز اطلاعات می تواند به طور محدودی تأثیرات منفی بر عملیات ها، دارایی ها یا اعضای سازمان وارد نماید.	**انسجام**- *حفاظت و جلوگیری از تغییر نادرست یا تخریب اطلاعات و از جمله تضمین انکارناپذیری [2] و اصالت اطلاعات*
تأثیرات منفی که ایجاد اختلال در دسترسی یا استفاده از اطلاعات بر امنیت کشور، عملیات ها، دارایی ها یا اعضای سازمان وارد می کند، می تواند شدید یا فاجعه بار باشد.	ایجاد اختلال در دسترسی یا استفاده از اطلاعات می تواند تا حد متوسط تأثیرات منفی بر عملیات ها، دارایی ها یا اعضای سازمان وارد نماید.	ایجاد اختلال در دسترسی یا استفاده از اطلاعات می تواند به طور محدودی تأثیرات منفی بر عملیات ها، دارایی ها یا اعضای سازمان وارد نماید.	**دسترسی پذیری**- *تضمین دسترسی و استفادهٔ بموقع و مطمئن از اطلاعات.*

[2]. انکارناپذیری یا nonrepudiation بدین معناست که کسی نتواند چیزی را انکار کند.

ضمیمهٔ 3- روش دسته بندی

مقیاس مکانی یا درجهٔ وضاحت (resolution) در ارائهٔ جزئیات اطلاعات جغرافیایی (مکانی) نقش مهمی ایفا می کند و درجهٔ حساسیت بسته به مقیاس یا وضاحت اطلاعات متفاوت می باشد. هر چقدر مقیاس بزرگتر باشد (برای مثال: 1:10،000)، ابعاد را می توان با جزئیات بهتر بیان نمود و دسته بندی اطلاعات حساس تر می شود). هر چقدر مقیاس کوچکتر باشد (برای مثال: 1:500،000)، ابعاد با جزئیات کمتر ارائه می شوند و همچنان حساسیت اطلاعات کمتر می شود).

جدول ذیل (متریکس مقیاس) حساسیت مجموعه های اطلاعات بنیادی جغرافیایی (مکانی) را بر مبنای میزان جزئیات ارائه شده بر حسب مقیاس های مختلف نشان می دهد و می بایست در دسته بندی اطلاعات در نظر گرفته شود. اطلاعات بر مبنای درجهٔ حساسیت شان که بر حسب مقیاس های متعدد ارائه شده اند، به دسته های عامه یا داخلی یا محرمانه تقسیم بندی می شوند. برای مثال، نقشهٔ توپوگرافیک افغانستان در مقیاس های 1:500 هزار، 1:250 هزار، 1:100 هزار و 1:50 هزار موجود می باشد و درجهٔ جزئیات آنها بسته به این مقیاس ها متفاوت می باشد. بنابراین، نقشهٔ توپوگرافیک در مقیاس بزرگتر و کوچکتر از 1:50 هزار با عنوان محرمانه دسته بندی می شود. نقشهٔ دارای مقیاس متوسط بین 1:100 هزار و 1:250 هزار با عنوان داخلی و نقشه های دارای مقیاس بزرگتر از 1:250 هزار با عنوان عامه دسته بندی می شوند.

درجهٔ جزئیاتی که در مقیاس های متعدد برای هر یک از مجموعه های اطلاعات بنیادی ارائه می شود، بسته به موضوع آن متفاوت می باشد و بنابراین دسته بندی آنها نیز متفاوت خواهد بود. برای مثال، اطلاعات شبکهٔ حمل و نقل جاده ای در مقیاس 1:250 هزار و بالاتر از آن در دسته بندی عامه قرار می گیرد، اطلاعات در مقیاس بین 1:50 هزار و 100 هزار در دسته بندی داخلی، و اطلاعات در مقیاس 1:25 هزار و پایین تر از آن در دسته بندی محرمانه قرار می گیرد.

بزرگ ← مقیاس → کوچک

		1m	500K	250K	100K	50K	25K	10K	5K	1K
1	محدوده های اداری									
2	جاده ها									
3	هایدرولوژی									
4	پوشش ارضی									
5	ساحات حفاظت شده									
6	جیولوژی									
7	مادل دیجیتلی ارتفاع (DEM)									
8	تصاویر اورتو/ماهواره ای									
9	نام های جغرافیایی									
10	نقشه های جغرافیایی									
11	نمره های زمین (تنها محدوده ها)									
12	نمره های زمین (اطلاعات شخصی)									
13	سرشماری									
14	تأسیسات عامه									

پوشش ارضی
داخلی
محرمانه
در دسترس نیست

نمودار گردشی ذیل جریان کار عمومی دسته بندی هر یک از مجموعه های اطلاعات بنیادی را نشان می دهد و تمام ادارات حکومت افغانستان باید این روند کاری را دنبال نمایند. این نمودار جزئیات مراحل کار را نشان می دهد اما مراحل کار به طور خلاصه قرار ذیل اند:

1. کار خود را با تعیین دسته بر مبنای مقیاس اطلاعات، طوریکه در متریکس مقیاس در بالا گفته شد، آغاز نمایید.
2. سپس دیگر عوامل مکمل از جمله موارد ذیل را در نظر بگیرید:
   - 2.1. ملاحظه نمایید که آیا اطلاعات حاوی معلومات شخصی می باشند یا خیر. معلومات شخصی به هرگونه جزئیات در مورد یک فرد یا کار اطلاق می شود.
   - 2.2. اگر اطلاعات حاوی هر گونه معلومات شخصی است، به درجهٔ جزئیات توجه داشته باشید، زیرا با این کار حساسیت اطلاعات مشخص خواهد شد. اگر اطلاعات، برای مثال، حاوی نام و تخلص یک فرد باشد، آنگاه درجهٔ حساسیت آن متوسط بوده و می بایست به عنوان اطلاعات داخلی در نظر گرفته شود. اما اگر اطلاعات

حاوی دیگر جزئیات شخص از جمله نام، آدرس، شماره تماس و غیره باشد، آنگاه حساسیت آن بسیار زیاد بوده و می بایست به عنوان اطلاعات محرمانه در نظر گرفته شود.

2.3. اگر اطلاعات حاوی معلومات شخصی نباشد، آنگاه ملاحظه نمایید که آیا اطلاعات در دسترس عموم قرار گرفته است یا خیر؛ به عبارت دیگر، آیا اطلاعات تاکنون توسط مالک آن در فضای عمومی انترنت منتشر شده است یا خیر. چنانچه اطلاعات هم اکنون در دسترس عموم قرار گرفته است، در آنصورت می بایست به عنوان اطلاعات عامه در نظر گرفته شود.

2.4. اگر اطلاعات در دسترس عموم قرار نگرفته است، با در نظرداشت هدف و محتوای آن تشخیص دهید که آیا اطلاعات حاوی جزئیات در مورد امنیت، اقتصاد و جمعیت می باشند یا خیر. اگر اطلاعات حاوی این جزئیات است، در آنصورت ملاحظه نمایید که آیا اطلاعات جدید و بروز (up-to-date) است یا خیر. اگر اطلاعات بروز بود، باید آنرا محرمانه تلقی نمایید، در غیر آن اطلاعات باید داخلی در نظر گرفته شوند.

2.5. اگر اطلاعات حاوی جزئیات در مورد امنیت، اقتصاد و جمعیت نبود، آنگاه ملاحظه نمایید که آیا اطلاعات جدید و بروز است یا خیر. اگر اطلاعات جدید و بروز بود، باید آنرا محرمانه تلقی کنید، در غیر آن اطلاعات باید عامه در نظر گرفته شوند.

3. بعد از اینکه سطح دسته بندی اطلاعات را با درنظرداشت عوامل مکمل تعیین نمودید، آنگاه می بایست ملاحظه نمایید که آیا این دسته بندی با دسته بندی های موجود در متریکس مقیاس (در جدول بالا) مطابقت دارد یا خیر. اگر مطابقت داشت، آنگاه اطلاعات و اطلاعات کلان آن را در دسته های مناسب قرار دهید و سپس آن را منتشر نمایید.

4. اگر با دسته بندی های موجود در متریکس مقیاس مطابقت نداشت، آنگاه ملاحظه نمایید که آیا سطح دسته بندی ارتقاء داده شده یا تنزیل یافته است. در صورتی که هر گونه تغییر در سطح دسته بندی اطلاعات بوجود آمده باشد، قبل از دسته بندی جدید و انتشار اطلاعات ضروری است تا تصدیق مدیر کسب گردد.

نمودار گردشی برای نمایش روش دسته بندی اطلاعات: