جمهوری اسلامی افغانستان
وزارت امور داخله
معینیت پالیسی و استراتیژی
ریاست عمومی پلان و پالیسی

طرزالعمل مخابره

و تکنالوژی معلوماتی

شماره ثبت: ۹۵
تاریخ منظوری: جوزا ۱۳۹۷
تعداد صفحات: ۷۷

فهرست مطالب

امر نخستین

افغانستان در یک ونیم دهه اخیر، دسترسی بی سابقه به تکنالوژی وفناوری مدرن پیدا کرده است که این مسله در کنار سایر موضوعات برای حکومت و شهروندان کشور حایز اهمیت میباشد. وزارت امور داخله و پولیس ملی منحیث مرجع نخست نظم وامن عامه و تنفیذ قانون نیازمند است تا گام های اساسی را در استفاده از تکنالوژی و فناوری مدرن بخاطر عرضه خدمات با کیفیت وسریع، مبارزه با انواع جرایم، تجهیز پولیس ملی و ادارات وزارت امور داخله با امکانات و تکنالوژی عصر نوین بردارد.

در شرایط کنونی، وزارت امور داخله از ابزار وسایل عصری استفاده مینماید، اما با توجه به ضرورت های فوق و مؤثریت تکنالوژی در حکومتداری خوب، هنوز وزارت داخله و پولیس ملی بصورت درست تجهیز واکمال نشده است. ایجاب می نماید که در پرتو قوانین، مقررات و پالیسی های جمهوری اسلامی افغانستان از امکانات مدرن در حوزه حکومتداری الکترونیکی استفاده بهینه صورت گیرد، روی این ملحوظ وزارت امور داخله و پولیس باید در بخش های مختلف این ارگان از تکنالوژی و فناوری عصری استفاده و نیز آنرا در حد بلندی گسترش بدهد.

طرزالعمل دست داشته، مطابق هدف سوم پلان استراتیژیک چهار ساله؛ روی سه محور اساسی، مشمول تجهیز ادارات واستفاده از امکانات جدید در راستای تنظیم وانسجام بهتر امورمربوط به ارائه خدمات سریع و معیاری، تجهیز و رفع نیازمندی ها وتوقعات قوای پولیس ملی در بخش مخابره و تکنالوژی عصری وظرفیت سازی به منظور حمایه ارتباطات استراتیژیکی، تاکتیکی و هدفمند بین ادارات و جزوتام های قوای پولیس، تاکید مینماید.

شایان ذکر است، ارایه خدمات به موقع مخابروی به منظور تأمین ارتباطات در وظایف، عملیات ها وامور روز مره پولیس ملی که درنهایت به حصول اهداف معین استراتیژیک وزارت امور داخله وپلان پولیس ملی منجر خواهد شد، اهمیت وجایگاه تکنالوژی ارتباطات را بیشتر از پیش برجسته نموده و تسهیلات مناسب تخنیکی را برای پرسونل پولیس ملی فراهم می سازد.

ضمن قدردانی از تیم بازنگری طرزالعمل مخابره و تکنالوژی به تمام ادارات زیربط و جزوتام های پولیس ملی امر مینمایم که جهت تطبیق وتحقق بلا انحراف طرزالعمل از هیچ گونه سعی و تلاش دریغ نورزند.

ویس احمد برمک

وزیر امور داخله

مقدمه

طرزالعمل هذا یک سند اجرایی در امور مخابرات و تکنالوژی معلوماتی برای منسوبین پولیس ملی وکارکنان ملکی وزارت امور داخله که توسط کارشناسان مجرب وبه همکاری ریاست عمومی مخابره و تکنالوژی و ریاست عمومی پلان و پالیسی مرور وتدوین گردیده است. این سند شامل مقدمه، تعریف اصطلاحات، شرح طرزالعمل، اساسات عمده ارتباطات در پنج فصل و 9 ضمیمه ترتیب شده است. در فصل نخست، مسئله تکنالوژی معلوماتی، شرایط فعال سازی وتوسعه شبکه، طرز معاینه و کنترول استندرد های بعد از تکمیل کار توسط شرکت قراردادی، مرکز معلومات، استفاده و نظارت از دوربین مداربسته به بحث گرفته شده است. فصل دوم مسایل مربوط به امنیت سایبری، ایجاد حساب برای کاربر ونحوه استفاده از اطلاعات، مسئله فعالیت ممنوع در سیستم و شبکه، رمز، مصونیت سرورها، دسترسی از راه دور به کمپیوترها، شرایط استفاده از انترنت به شمول مدیریت نرم افزار ها توضیح یافته است.

در فصل سوم، سیستم مدیریت معلومات، بانک معلومات، خدمات الکترونیکی، امنیت داده ها و سیستم ها، ظرفیت سازی مدیریت و کارکنان سیستم، ترتیب وایجاد امنیت بانک معلومات به بحث گرفته شده است. فصل چهارم حاوی ارتباطات تاکتیکی، مسؤلیت های مراکز مخابره، پروسه ااستندرد عملیات، توسعه پروتوکل های مشترک، محرم سازی ارتباط شفری، سیستم اداره منابع ارتباطی ومعلومات اشد محرم میباشد. فصل پنجم پروگرام های حمایوی و تعلیمات مسلکی، دوره حیات، اجناس ووسایل مصرفی، بودجه وقرارداد، سوق واداره مخابره سیم دار، کمره امنیتی، شبکه جزوتام ها، رهنمود استفاده از صلاحیت نظارتی و واگذاری مسؤلیت ها و مسؤلیت های ادارات وضمایم وفورمه های استفاده رسمی این طرزالعمل به تفصیل بیان شده است.

توقع میرود با تطبیق و تحقق این طرزالعمل گامی اساسی بطرف اصلاحات و تغییر مثبت در راستای استفاده از مخابره و تکنالوژی مدرن در وزارت امور داخله برداشته شود.

هدف

هدف از مرور طرزالعمل مخابره و تکنالوژی معلوماتی عبارتند از:

- تدوین سند رهنمودي به منظور تنظیم وانسجام بهتر امور ریاست عمومی مخابره و تکنالوژی معلوماتی به اساس تنظیم تشکیلاتی سال 1396
- توسعه قابلیت های معاصر تخنیکی و تکنالوژیکی به منظور کنترول وضعیت، دفع تهدیدات و کاهش تلفات پولیس
- تحلیل و ارزیابی پلان ها از دید امنیتی و عملیات های کشفی و استخباراتی پولیس
- تعویض سیستم های کلاسیک اجرائی با سیستم های الکترونیک معاصر
- ایجاد ذخیره گاه ها و بانک های معلوماتی با ظرفیت های وسیع و متناسب با نیازمندي های ادارات پولیس
- ایجاد سیستم های کنترول الکترونیکی از فعالیت های روزمره ادارات پولیس
- ایجاد طرزالعمل تطبیقی در بخش امنیت سایبری
- ایجاد سیستم های شفاف در شبکه ارتباطات استراتیژیک میباشد.

ساحه تطبیق

این طرزالعمل در تمام سطوح تشکیلات قواي پولیس و سایرادارات شامل تشکیلات وزارت امور داخله که از وسایل مخابروي و تکنالوژی معلوماتی استفاده مینمایند و نیز ادارات ذیربط که در طرزالعمل موجوده مشخص گردیده قابل تطبیق می باشد.

تعریف اصطلاحات

شبکه (Network)	ارتباط حداقل دو وسیله (کمپیوتر) را شبکه کمپیوتری گویند.
تکنالوژی معلوماتی (Information Technology)	کلمه یونانی است به معنی علم، تخنیک ومعلومات استـفاده شده است.
پروسیجر (Procedure)	طرزالعمل روش مرحله به مرحله.
پورت یوایس بی (Universal Serial Port)	محل اتصال چیپ (فلش) ویا حافظه
تلیفون وایپ (Voice over IP)	تیلیفونهای که ازطریق پرتوکول یا آی پی (شبکه) انترنت طورمحرم کارمیکنند
نام کاربر (User Name)	مشخصه که برای کاربر کمپیوتر(شبکه) وسیستم های معلومات استفاده میشود
حساب کاربر (User Account)	نام یا حساب شخص که به اساس آن به سیستم دسترسی پیدا میکند
لگ آف (Log off)	بسته کردن حساب بازشده کاربر.
کیبلینگ (Cabling)	کیبل دوانی لین های ارتباطی شبکه
کت (Cat)	نوع ازکیبل های ارتباط شبکه است.
دکت (Duct)	مجرای کیبل ها به منظورحفاظت کیبل ها است.
رك (Rack)	صندوق که عموماً به منظور جابجا کردن سویچها استفاده میشود.
فایبرنوري (Fiber Optic)	کیبل به خاطر انتقال سریع دیتا استفاده میگردد
وال جک (Wall Jack)	مانند ساکت برق دیواري بوده به منظور اتصال کمپیوترها، تیلیفونها ووسایل دیگرشبکه استفاده میشود
وایس ودیتا (Voice and Date)	سیستم صدا (تیلیفون) وسیستم معلومات کمپیوتر میباشد
ستیکر (Sticker)	علایم چاپی به منظورمشخص ساختن وشناسایی وسایل است
ورانتی (Warranty)	خدمات بعد ازفروش وسایل میباشد
آنلاین (Online)	زنده یا هم زمان فعال
سایت (Site)	بخش (یک ساحه جداگانه که به شبکه وصل شده).
سرور (Server)	وسیله شبه کمپیوتراست که خدمات را ارایه وتنظیم مینماید
کانفگریشن (Configuration)	عمل تنظیمات وعیارسازي وسایل
نصبیشن (Installation)	پروگرام کردن یا نصب کردن نرم افزارها.
ایمیج (Image)	کاپی گرفتن تمام تنظیمات و فایل ها از کمپیوتر
ویندوز مایکروسافت (Window Microsoft)	پروگرام اساسی فعالیت کمپیوترها وسرورها تولید شرکت مایکروسافت میباشد
ورژن (Version)	نسخه ازتولید یا نوع تولید
کمپلکس(Complex)	ترکیبی (پیچیده).

سی دي روم (CD-ROM)	محل نصب وخواندن سی دي در داخل کمپیوتر است
ویروس(Virus)	میکروب که وسایل تکنالوژی معلوماتی وارتباطی را آلوده میسازد
آنتی ویروس(Anti-Virus)	پروگرام ضد میکروب که وسایل تکنالوژی معلوماتی وارتباطی آلوده را پاك میکند
اسکن (Scan)	عکس برداري از فایل توسط پرنتر بررسی کردن
فارمت (Format)	شکل
درایو (Drive)	قسمت ازحافظه هارد دسک است
مسنجر (Messenger)	وسیله که برای اخذ وارسال پیام وصحبت کردن استفاده می شود
مدیا پلیر(Media player)	نرم افزاری که که قادر به خواندن ویدیو، تصویر و صدا است
شبکه ناك (Network Operation Center)	مرکزعملیات فعالیت های شبکه وزارت امور داخله است
دیتابیس(Date Base)	بانک مرکز اطلاعات.
اهریمز (AHRIMS):	سیستم ثبت منابع بشری (سوانح الکترونیکی) وزارت امور داخله
آی پی ایس (Intrusion prevention systems)	سیستم جلوگیري ازورود برنامه های غیرمجازبه شبکه
دیتا (Data)	اطلاعات گسسته و خام که بااستفاده از وسایل تکنالوژی معلوماتی وارتباطی جمع آوري میشود
سرورپالیسی (Server Policy)	پالیسی های که ازطریق سرورها بالای حساب کاربران اعمال می شود
فایروال(Firewall)	وسیله که به منظور امنیت شبکه استفاده میشود
ویدیوکنفرانس (Video Tele Conference)	کنفرانس (جلسه) صوتی و تصویري از راه دور
منابع معلوماتی (Information Resources)	شامل ثبتیات، ریکارد ها ومعلومات که ازطریق سیستم های تکنالوژی معلوماتی قابل دسترسی باشد
ریکارد (Record)	ثبت معلومات درمورد یک شخص یا چیز واحد
دیتاسنتر (Data Center)	مرکز معلومات یا جای که تمام اطلاعات ومعلومات الکترونیکی ذخیره واستفاده میشود
هاردویر(Hardware)	شکل فزیکی وسایل سخت افزار
سافت ویر(Software)	نرم افزارشکل منطقی پروگرام وسایل
کود (Code)	شفربه شکل محرم
کف کاذب (Raised Floor)	سطح دومی که بالای زمین در دیتاسنتر ساخته میشود
ای سی اس سرور(ACS Server)	وسیله شبکه است که به خاطر امنیت وسایل شبکوی استفاده میگردد
HVAC(Heating, ventilation, and air conditioning)	سیستم خنک کننده و تهویه هوا میباشد.

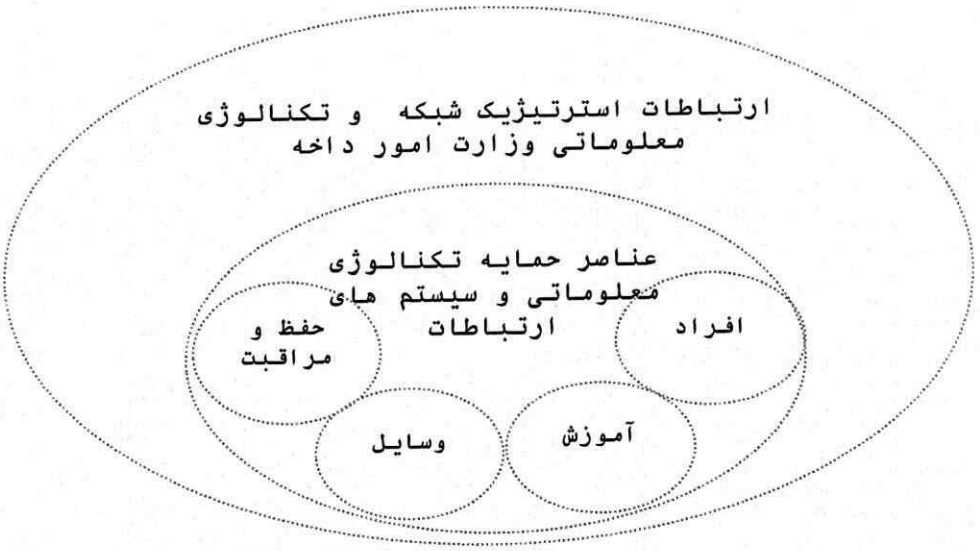
تلنت و اس اس اچ Telnet و SSH	دو پروتوکول که به خاطر دسترسی از راه دور استفاده میگردد.
فست ایترنت Fast Ethernet	پورت فست ایترنت وسیله انتقال دیتا میباشد.
ان وی رم NVRAM	حافظه دایمی روتر میباشد که عیارسازی در آن ذخیره میگردد.
آتنتیکیشنAuthnetication	از طریق این میتود تثبیت هویت میگردد
مسیر منبع Source route	مسیر آمدن پاکت ها در شبکه یا مبدا را نشان میدهد
دی ام زی DMZ	بخش هایی از شبکه که کاملا قابل اطمینان نیست.

چالش ها

- فقدان روشهای تأمین امنیت وسایل شبکوی سایبری وزارت اموراخله در طرزالعمل قبلی
- تعویض متوازن سیستم های کلاسیک اجرایی با سیستم های الکترونیک معاصر
- عدم موجودیت ایجاد ذخیره گاه ها وبانک های معلوماتی با ظرفیت های وسیع و متناسب با نیازمندي های ادارات وزارت امور داخله
- نبود سیستم منظم تحلیل و ارزیابی پلان ها از دید امنیتی وعملیات های کشفی واستخباراتی پولیس
- عدم موجودیت سیستم های لازم کنترول الکترونیکی از فعالیت های روزمره ادارات وزارت اموراخله.

شرح طرزالعمل

شکل ذیل عناصر حمایوي ریاست عمومی مخابره و تکنالوژی معلوماتی را نشان میدهد.



اساسات عمده تأمین ارتباطات

تأمین ارتباطات بین قدمه ها و سایر ارگانهای ذیربط دوامدار بوده محدود به محدوده زمانی(رخصتی و رسمی) نمی باشد.

تأمین ارتباط محدود به فاصله وساحه نبوده صرف نظر ازساحه دور یا نزدیک، حضر و سفر در هرنوع شرایط باید تأمین باشد.

متکی بودن به یک نوع وسیله تأمین ارتباط ممکن مشکلات را بوجود بیاورد، بناً لازم است تا با استفاده از وسایل و روش های مختلف، علاوه بر وسیله ارتباط اصلی، وسیله ارتباطی احتیاطی ۱، ۲ وحتی ۳ و۴ را نیز مد نظر گرفت. محرمیت و شفافیت ارتباطات منحیث یک اصل اساسی باید حفظ و رعایت گردد.

پرسونل بخشهای تأمین ارتباطات، امکانات و تسهیلات کافی و مناسب را دردسترس داشته باشد تا دراجراات شان سکتگی رونما نگردد.

مکالمات (تماس های سیمدار و بیسیم) مختصر، کوتاه و پرمحتوا باشد. اخذ وارسال مطالب با دقت و اصول صورت گیرد تا ازسکتگی دراجراات جلوگیري بعمل آمده بیاید. ارسال کننده و اخذ کننده پیام ها طور مسئولانه پیام ها را از نگاه درجه بندي محرمیت و استعجالیت طبقه بندي نموده تا اجراکننده طبق آن اجراات نماید.

فصل اول

تکنالوژی معلوماتی

شرایط فعال سازی و توسعه شبکه تکنالوژی معلوماتی

برای جلوگیری از مصارف بی مورد منابع، اتلاف وقت، و استفاده بهینه از سیستم لینی شبکه تکنالوژی معلوماتی وزارت امور داخله، برای فعال سازی و توسعه شکبه تکنالوژی معلوماتی شرایط ذیل باید در نظر گرفته شود:

- تعمیر ملکیت دایمی وزارت اموراخله باشد.
- پلان تخریب یا بازسازي آن مطرح نباشد.
- موجودیت پرسونل در تاسیسات موقتی نباشد.
- سیستم انرژي برق ازطریق شبکه برق شهري و یا جنراتور طور ثابت ودوامدار تهیه شده بتواند.
- تمام اطاق های تعمیر که به منظور دفاتر و اطاق های کنفرانس و یا صنوف درسی استفاده میشوند باید سهولت پورت (کنکشن) وصل ساختن کمپیوترها نظر به تعداد کارمندان، وهردفتریک کنکشن برای اتصال تیلیفون وایپ داشته باشد(یک تیلیفون برای استفاده چند تن و کمپیوتر برای هر کاربر طورجداگانه در داخل یک دفتر) مدنظرگرفته شود.
- فورم سروي (درخواست ساحه) ازطریق افسرمسئوول یا آمرمخابره و تکنالوژی معلوماتی درهماهنگی با بخش ریاست تسهیلات با منظوري آمر(قوماندان) جزوتام ترتیب و با درنظرداشت شرایط فوق خانه پوري و به مدیریت ارتباطات استراتیژیک معلوماتی ریاست عمومی مخابره و تکنالوژی معلوماتی ارسال میگردد.
- درساحات که قبلا شبکه فعال شده باشد آمرین مخابره درخواستها را طور انفرادي برای یک یا چند کنکشن ارسال نمی نمایند. تمام درخواستها (نیازمندي ها) را جمع آوري، سروي و ارزیابی کرده و فورم توحیدي درخواست ساحه را خانه پوري نموده به مدیریت ارتباطات استراتیژیک معلوماتی ارسال مینماید.

مدیریت ارتباطات استراتیژیک بعد از ارزیابی طبق هدایت مسئوولین ریاست عمومی مخابره و تکنالوژی معلوماتی با درنظرداشت اولویت ها، تصمیم اتخاذ وپلان اجرائیوي فعالسازي وتوسعه شبکه را در ساحه مورد نظرترتیب مینماید.

تمام وسایل و تجهیزات مطابق تعداد کنکشن ها (پورت ها) موجود از طریق مدیریت اکمالات ریاست عمومی مخابره و تکنالوژی معلوماتی توزیع می گردید. آمر مخابره و تکنالوژی با مشوره قوماندان یا آمر مربوطه به منظور جلوگیري از اتلاف وسایل و طرزاستفاده معقول ازآن ها پلان توزیع وسایل را ترتیب مینماید که در آن سنجش هرشعبه صورت میگیر، مثلاً اگر در یک شعبه کنکشن های متعددی برای اتصال تیلیفون موجود باشد و تنها یک تیلیفون کافی باشد، تیلیفونهای متباقی درخواست شده در دیپو مربوطه نگهداري میگردد. کمپیوتر برای هر منسوب دفتر با درنظرداشت تشکیل حتمی بوده و طبق کنکشن(پورت دیتا) از بالا به پایین توزیع میشود.

ازیک کمپیوتر دو یا چند تن به شرطی استفاده کرده میتوانند که هرکدام (نام کاربر) اسم کاربر جداگانه داشته وهرکدام بعد از استفاده کمپیوتر را (لگ آف) نیمه خاموش مینماید تا شخص دیگرازطریق نام کاربر صرف به اسناد خویش دسترسی پیدا کند نه به اسناد و بخش شخص دیگر (در صورت استفاده نمودن از یک کمپیوتر مسئوول میز کمک را در جریان گذاشته تا مقدار فضای کافی را برای هر شخص بصورت جداگانه اختصاص دهد).

کمپیوترها به افسران، ساتنمنان و مامورین توزیع میشود که تعلیمات کامل و یا ابتدایی تکنالوژی معلوماتی را فرا گرفته و از آن استفاده معقول کرده بتوانند، درغیرآن وسایل بطورموقت در دیپو نگهداري می شود.

براساس پالیسی و پروسیجر عمومی زمانیکه تعمیر در تطابق باشرایط فوق باشد به جز از اطاق های که برای دیپوها، اطاق های استراحت (کاغوش ها) آشپزخانه مشخص گردیده باشد در متباقی اطاق ها لین دوانی (کیبلینگ) صورت میگیرد تا درآینده ازمصارف بی جا و مکرر جلوگیري شود.

طرز معاینه و کنترول استندردها بعد از تکمیل کار

درختم کارکیبلینگ (لین دوانی) و توزیع وسایل در مرکز از طرف مسئوولین شبکه و در ساحه از طرف مسوولین مدیریت های مخابره و تکنالوژی معلوماتی کنترول ومعاینه استندردهای ذیل صورت گیرد:

- تمام دراپ ها (کنکشن ها) توسط آله چک کننده کمپیوتر وتیلیفون عملاً چک وکنترول گردیده وازفعال بودن آن اطمینان حاصل گردد.
- ملاحظه شود که تمام کیبل های (کت5 یا6) شبکه داخل دکت ها (پوش محافظوي) بوده و از ایجاد خلاها و درزهای که باعث رسیدن آسیب ها وضررهای احتمالی حیوانات وحشرات به کیبل ها میگردد جلوگیري بعمل آید.
- کیبل های شبکه از لین های برق مجزا ومحفوظ باشد تا ازوقوع شارتی و حریق احتمالی جلوگیري گردیده باشد.
- راك ها (آلماریها) به منظورجابجا کردن سویچها درمحلات محفوظ و بیخطر، و دور از تماس با دروازه ها و سایر موانع بوده وسبب ایجاد مزاحمت ومشکلات برای پرسونل مربوطه نگردد.
- وال جک ها از تصادم با دروازه ها وچوکی ها محفوظ باشد.
- کیبل های فایبرنوري طبق استندرد در زیر زمین جدا از کیبل های برق تمدید شود تا از خطر حریق وسایر آسیب ها در امان باشد، و همچنان نقشه آن ترتیب شده و یک نقل آن به بخش تعمیرات ونقل دیگرآن دربخش تکنالوژی معلوماتی وشبکه نگهداري شود.
- تمام وال جک های (صدا و دیتا)، ستیکر با شماره های مشخص داشته باشند همچنان به کیبل که به سویچ وصل گردیده باشد عین شماره مطابقت داشته باشد.
- تمام وسایل طبق مشخصات چک وکنترول شده ثبت دفاتر شوند.
- ایمل آدرس و شماره تماس مرجع ورانتی کننده درج اسناد شده تا درصورت بروز مشکلات و عوارض بدون ضیاع وقت با آنها تماس حاصل شده بتواند.

برنامه های نظارت کننده (Monitoring Software)

استفاده از نظارت کننده ها باید به صورت ذیل باشد:

- استفاده ازابزارهای مانند LAN Analyzer (تحلیل کننده شبکه) و Packet Sniffer (نگارنده پاکت های معلوماتی) محدود به مدیریت شبکه بوده و کسی دیگر حق استفاده را ندارد.
- در صورت عدم ضرورت باید این ابزارها به صورت امن نگهداری شود.
- به خاطر شناسایی دسترسی های غیر مجاز باید Intrusion Detection System عیار سازی گردد.
- درهر وسیله شبکه باید توسطACS(Access Control Server) عیار سازی گردیده تا دسترسی های غیر مجاز شناسایی گردد.

ساحه تطبیق

هر کارمند وزارت درصورت تخطی از مواد این طرزالعمل با اقدام انظباطی مواجه شده که حتی موجب به سبکدوشی از وظیفه خواهد شد.

پروسه اجرای وظایف شرکت قراردادی

شرکت برنده در پروسه تدارکات بعد ازطی مراحل قانونی در روشنی احکام قانون تدارکات با بخش از خدمات ارتباطی عقد قرارداد مینماید. سند قرارداد را به ریاست عمومی مخابره و تکنالوژی معلوماتی به عنوان معرفی نامه و طی مراحل اداري طور محفوظ می سپارد.

ریاست عمومی مخابره وتکناولوژي معلوماتی درابتدا مرجع نیازمند (فرمایش دهنده) و شرکت قراردادي (فرمایش گیرنده) را شناسایی واطمینان حاصل می نماید. متعاقباً شرکت قراردادي کاپی تذکره تابعیت و یا پاسپورت، فورم ضمانت و دو قطعه عکس کارمندان را بریاست عمومی مخابره و تکنالوژی معلوماتی ارسال می نماید..

ریاست مخابره و تکنالوژی معلوماتی اسناد متذکره را به منظورتثبیت هویت ومعلومات ازمسئوولیت وعدم مسئوولیت آنها بریاست مبارزه با جرایم جنائی ارسال مینماید.

ریاست مبارزه با جرایم جنائی بعد از بررسی درمورد مسئوولیت وعدم مسئوولیت افراد مورد نظربریاست مخابره معلومات دقیق را ارایه می نماید. ریاست عمومی مخابره و تکنالوژی تمام این معلومات را که رفع مسئوولیت شده باشد حفظ نموده برویت آن جواز کار برای کارمندان شرکت درمربوطات وزارت اموراداخله میدهد.

درصورت جذب کارمند جدید پروسه فوق طور انفرادي تطبیق میگردد.

قراردادي بعد از طی مراحل فوق لیست عمومی کارمندان خویش را با توضیح شهرت به ریاست عمومی مخابره ارسال مینماید. توظیف، تغییر وتبدیل درمحل کار، کارمندان شرکت نیز به ریاست عمومی مخابره خبرداده می شود.

ریاست عمومی مخابره به استناد سند فوق موضوع را به مرجع که کاردر آن جریان دارد رسمن اخبار و درحصه معرفی کارمندان جدید نیز اجراات می نماید.

مرجع مذکور(محل وظیفه) سند متذکره را حاصل نموده و به کارمندان اجازه دخول و کار را طبق قواعد ومقررات میدهد.

درصورتیکه کدام یکی ازکارمندان وظیفه محوله را ترك مینماید شرکت قراردادي مکلف است تا جواز شناسایی وزارت امور داخله را از نزدش استرداد و به ریاست عمومی مخابره و تکنالوژی با توضیح موضوع تسلیم نموده، و از شعبه یا اداره مربوطه که همراه اش همکاري یا مسئوولیت داشته سند عدم مسئوولیت حاصل نماید تا درآینده از ناحیه مسایل اداری و امنیتی مشکل ایجاد نشود.

شرکت هایی که در بخش ارتباطات شبکه و تکنالوژی معلوماتی عقد قرارداد مینمایند تحت نظارت ریاست عمومی مخابره و تکنالوژی معلوماتی ودرساحات تحت نظرآمرین مخابره و تکنالوژی معلوماتی جزوتامها فعالیت مینمایند.

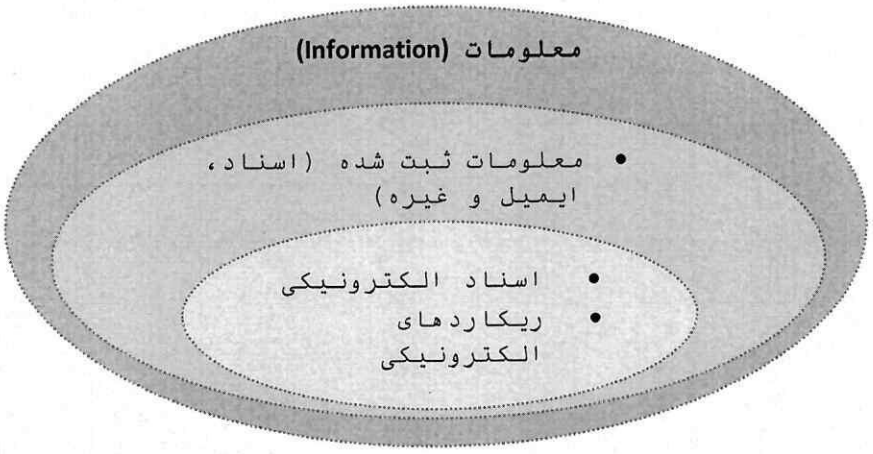
طرز حسابدهی و جوابگویی شرکت های قراردادي به ارگان های دولتی مطابق به قوانین نافذه کشور بوده و مطابق آن جبران خساره وبررسی ها صورت میگیرد.

دیتاسنتر یا مرکز معلومات

دیتاسنتر برای پیشبرد عملیات وزارت امور داخله بسیار مهم و حیاتی میباشد. پالیسی و روش های ذیل به خاطر اطمینان از امنیت وقابلیت اطمینان سیستم های موجود در دیتاسنتر میباشد. تهیه و ترتیب هدایت و رهنمود برای دیتاسنتر، نصب و راه اندازی، حذف ودفع تجهیزات، کنترول دسترسی به صورت فیزیکی و امنیتی، ایمنی، درخواست برای خدمات و یا منابع خاص، درخواست مکان، مدیریت سیستم برق، مدیریت لین ها، تعمیر ونگهداری و پاکیزگی محل کار به صورت عمومی و دیگر اقلام متفرقه در داخل دیتا سنتر میباشد.

تنظیم و اداره منابع معلوماتی

منابع معلوماتی پولیس ملی وزارت اموردا‌خله افغانستان یک منبع با ارزش بوده که باید مانند سایرمنابع (بشری، بودجه واجناس) حفظ، نگهداري وتنظیم شود. این منابع معلوماتی شامل ثبت، ریکاردها، دیتابیس ها، دوسیه ها وسایراسناد ومعلومات میباشد.



در شکل بالا معلومات به حمایه دیتابیس ها و یا به شکل انفرادي و غیره سیستم ها ازطریق مسئوولین مربوطه به حمایه وسایل با استفاده از تجهیزات تکنالوژی جمع آوري شده وتوسط سرورها و وسایل تکنالوژی معلوماتی حفظ و ذخیره میشوند که امکانات شریک ساختن، تغییردادن واضافه کردن درآن میسرنباشد.

- معلومات مذکور طورآزادانه به دسترس هرمنسوب وزارت اموردا‌خله یا افراد جامعه قرارنمی گیرد مگر برویت سند صلاحیت که ازنگاه وظیفه مسوولیت آن رامشخص میسازد .
- صلاحیت دسترسی به معلومات نیز صنف بندي میگردد مانند: صلاحیت صرف مطالعه، صلاحیت مطالعه وآوردن، صلاحیت حذف نمودن، صلاحیت اضافه کردن و شریک ساختن برویت فورم مشخص.
- ریاست عمومی مخابره و تکنالوژی معلوماتی علاوه بر وظایف اصلی در بخش تنظیم اداره منابع معلوماتی نیز مسئوولیت داشته و منحیث مسئوولین با صلاحیت در بخش تنظیم امور متذکره به مقامات و رهبري وزارت امور داخله یاري می رسانند.
- درسطح تشکیلات ساحوي، آمرمخابره و تکنالوژی معلوماتی و یا منسوب دیگري از طرف آمرین و یا قوماندانان مربوطه منحیث افسرموظف تنظیم کننده معلومات تعیین و پیشنهاد اش را به ریاست عمومی مخابره و تکنالوژی معلوماتی غرض منظوري و تعیین و تفویض صلاحیت ارسال مینماید.

- ریاست عمومی مخابره و تکنالوژی معلوماتی سیمینار مشخص را به مسئوولین تنظیم منابع معلوماتی پلان و راه اندازي مینماید.
- جمع آوري، ثبت، تغییر، نشر و شریک ساختن معلومات از جمله وظایف مسئوولین ثبت ریکارد جزوتامهای مختلف وزارت امور داخله بوده و تنها موضوع ذخیره و حمایت ازطریق وسایل تکنالوژی بدوش مدیریت دیتاسنتر ریاست عمومی مخابره و تکنالوژی معلوماتی می باشد.

روشهای دسترسی به دیتاسنتر

به منظوراطمنیان از نگهداری مطمئن و امن سیستم هایی که در دیتاسنتر موجود میباشد، روشهای ذیل به تمام کسانی که ضرورت به دسترسی دارند قابل تطبیق میباشد.

- تمامی اشخاصی که به دیتاسنتر دسترسی دارند باید دارای مجوز مخصوص (کارت دخول) باشند. اشخاص بدون مجوز مخصوص به حیث بازدید کننده شناخته میشوند.
- بازدید کننده گان از دیتاسنتر درصورت داشتن اجازه نامه (مکتوب) باید توسط مسئوول دیتاسنتر همراهی گردند.
- تمام اشخاص باید کارت هویت وزارت داخله یا شرکت های قراردادی را بصورت قابل دید بپوشند.
- تمام اشخاص هنگام ورود و خروج به دیتاسنتر باید هدف و زمان بازدید از دیتاسنتر را در فورم نوشته و امضا کنند.
- اشخاص مجاز(دارنده کارت دخول) اجازه ورود به دیتاسنتر را در هر زمان داشته میباشند ولی هدف وزمان مورد را نوشته نمایند.
- سیستم هایی که در داخل دیتاسنتر جابجا گردیده و حاوی معلومات مهم طبقه بندی شده باشد باید توسط کارمند دیتاسنتر از طریق کمره ها به صورت زنده نظارت گردد و کمره های متذکره باید ویدیو را ثبت نموده تا در صورت بروز مشکل به آن رجوع کنند.

تجهیزات در داخل دیتاسنتر

در تلاش برای به حداکثر رسانیدن امنیت و به حداقل رسانیدن اختلالات روشهای ذیل به تمام تجهیزات مستقر در دیتاسنتر قابل تطبیق است.

- به خاطر نصب، برداشتن یا تغییر آوردن تجهیزات باید ثبت و راجستر کتاب تجهیزات شبکه ناک گردد.
- کارمند دیتاسنتر باید مانع کارمندان مجاز یا قراردادی های دیگر به خاطر نصب یا دور کردن یا تغییر نام دادن تجهیزات بدون فورم دقیق تجهیزات گردد.
- تجهیزات مستقر در داخل دیتاسنتر باید مطابق مشخصات دررک ها(الماریهای) مشخص مربوطه قرارگیرد.

ضروریات ایمنی

کاشی های کف نباید بدون اجازه مدیر بخش مربوطه یا یکی از اعضای تیم خود خذف یا برداشته شود. اگر کاشی های کف برداشته می شود، فضای باز باید توسط مخروط ها یا نوار ایمنی محاصره شود. نباید بیشتر از دو کاشی به هم پیوسته در عین زمان باز باشد. با توجه به فشار طبقه تحتانی، تعداد کاشی های کشیده شده باید به حداقل رسانیده شود. همه کاشی های برداشته شده دو باره به موقعیت اصلی به شکل درست برگردد.

تمام دروازه های رکها(الماریها) باید درهر زمان بسته باشد مگر اینکه درحال استفاده باشند.

تغییرات در سیستم برق دیتا سنتر باید توسط متخصص برق با صلاحیت انجام شود. هر گونه تغییر باید با هماهنگی کارمندان دیتاسنتر و یا مدیر دیتاسنتر صورت گیرد. آزمایش برق باید با اجازه قبلی از مدیر دیتاسنتر برنامه ریزی شود.

هیچ کاری نباید در زیر ساحه کف کاذب (Raised Floor) بدون تایید مدیر دیتاسنتر صورت گیرد.

اگرهشدار به وسیله سیستم شناسایی دود (Smoke Detection System) در داخل دیتاسنتر فعال گردد باید پلان تخلیه اضطراری (Fire Emergency Evacuation Plan) ساختمان ها تطبیق گردد.

تهویه هوا و کیفیت هوای مورد نیاز

درجه حرارت در داخل دیتا سنتر باید به صورت ایده آل (20 درجه سانتیگراد) تنظیم و نگهداری گردد و یا همیشه بین 16-22 درجه سانتی گراد باشد.

همه سیستم های تهویه مطبوع دیتاسنتر و کنترل هوا که ضرورت جدی به عملکرد مناسب دارند باید قابلیت سرویس دهی را در هر زمان داشته باشند. سرویس تعمیر ونگهداری سیستم تهویه هوا باید هر سه ماه توسط کارمندان دیتاسنتر برنامه ریزی گردیده و درحالات عاجل به هیچ صورت سرویس تهویه هوا نباید محدود گردد.

مایعات تمیز کننده صنعتی یا هرنوع مایعات دیگر نباید در داخل دیتاسنتر ریخته یا مانده شود.

خوردن یا آوردن هر نوع غذا یا نوشیدنی به داخل دیتاسنتر جداً ممنوع گردیده است.

هیچ تغییری نباید درگرمایش، تهویه و سیستم های خنک کننده (HVAC) بدون در دست داشتن جواز از مدیر دیتاسنتر یا ریاست عمومی مخابره و تکنالوژی معلوماتی صورت گیرد.

وسایل جدید تعیین شده برای دیتاسنتر باید بیرون از دیتاسنتر از جعبه آن خارج گردد. درصورت موارد استثنا باید همراه جعبه آن در داخل دیتاسنتر باشد پس باید مراقب آلودگی آن بوده و بعد از خارج نمودن از جعبه توسط جاروب برقی پاک کاری گردد. نباید وسایل بسته در داخل دیتاسنتر بماند.

مراقبت کننده های سیستم های (HVAC) باید فعالیت های تعمیر و نگهداری سیستم های (HVAC) را بر اساس نیازمندی سایت مورد نظر برنامه ریزی کنند.

دسترسی وصلاحیت های مورد نیاز:

تمام دسترسی و صلاحیت های مورد نیاز به دیتا سنتر باید از "روشهای دسترسی به دیتاسنتر" که در فوق ذکر گردیده پیروی شود.

تغییر و تبدیل (Change Management Procedure)

تمام تغییرات و تبدیلات در داخل دیتاسنتر به شمول تغییرات درساختار، راه اندازی یا انهدام تجهیزات، برنامه های پیشگیری نگهداری، تعمیر تجهیزات درحالت اضطراری وآزمایش سیستم ها باید مطابق به پروسیجر مدیریت تغییرات (Change Management Procedure) ازقبل برنامه ریزی شده و با مدیر شبکه یا دیتاسنتر هماهنگی صورت گیرد.

تجهیزات سخت افزار دیتاسنتر مانند رک ها (الماریها) نباید بدون داشتن جواز از مدیر دیتاسنتر اضافه یا برداشته گردد.

مدیریت فضای موجوده در داخل دیتاسنتر مسئوولیت مدیر دیتاسنتر بوده و تمام پروژه های خاص باید همراه مدیر ارتباطات استراتیژیک یا دیتاسنتر هماهنگ گردد.

تمام تجهیزات باید قابلیت جابجای در داخل رک ها (الماریها) را داشته باشد و رکهایی که مورد استفاده قرار میگیرند باید توسط مدیر دیتاسنتر مشخص گردد. هرنوع استثنا باید توسط مدیر دیتاسنتر یا مدیر عمومی ارتباطات استراتیژیک تصویب گردد.

تجهیزات غیر قابل استفاده (Decommissioned Equipment)

برداشتن هرنوع وسایل که دوره حیات (Life Cycle) آن تکمیل گردیده باشد در هماهنگی با مدیر دیتاسنتر صورت گیرد.

مدیر دیتاسنتر میتواند تاریخی را با مدیر مربوطه تجهیزات غیر قابل استفاده هماهنگ نموده و برنامه ریزی نماید.

تمام تجهیزات که دوره حیات (Life Cycle) آن تکمیل گردیده باید درطول 60 روز تبدیل گردند.

تمام کیبل های ارتباطی دیتاسنتر که دوره حیات (Life Cycle) آن تکمیل گردیده به شمول صدا، دیتا، کیبل های فایبر نوری باید تبدیل گردند.

ضروریات رکهای شبکه و سرور

رک (الماری) سرورها باید به شکل محفظه بسته همراه با مکانیزم قفل مجهز باشد. رک های اااستندرد باید توسط مسئوول مدیریت عمومی ارتباطات استراتیژیک یا مدیریت دیتاسنتر تصویب گردد.

ضروریات برق

تنها شخص مسلکی برق با صلاحیت میتواند که پانل های الکتریکی یا واحد توزیع برق (Power Distribution Unit) را باز کند.

کیبل های برق زیر کف کاذب (Rise Floor) یا اتصال سرویس ها در دیتاسنتر نباید توسط افراد غیرمسلکی قطع یا وصل گردد.

کارمندان دیتاسنتر مسئوولیت قطع یا وصل نمودن سیم های برق تجهیزات زیر کف کاذب را به عهده دارند. وسایل و یا ابزار پاک کننده که به خاطر پاک کاری مورد استفاده قرار میگیرد باید به ساکت های برق عادی درداخل دیتاسنتر وصل گردد.

ضروریات کیبل های برقی برای وسایل جدید باید قبلا در دسترس مدیر دیتاسنتر قرار داده شود تا در هماهنگی با کارمندان دیتاسنتر یک منبع جدید برق برایشان تهیه و تعیین گردد.

از نوارچسپ (رابرتیپ) نباید در داخل دیتاسنتر استفاده گردد مگر به شکل موقت در زمان اضطراری استفاده شده میتواند.

نصب یو اس پی های ثانوی (احتیاطی) در داخل دیتاسنتر بدون آگاهی واستیذان مدیر دیتاسنتر صورت گرفته نمیتواند.

برچسب زدن نام و شماره گذاری (Labeling)

معلومات مربوط به برچسب کیبل ها، جهت رفع به موقع مشکلات باید بشکل کتبی جدول بندی و شماره گذاری شود.

تمام تجهیزات و سرورها باید به صورت خوانا و واضح برچسپ شود.

تمام رک ها و تجهیزات برق باید به صورت دقیق برچسپ زده شود، تا مشخص گردد که کدام لین برق به کدام فیوز متصل است.

جزییات تمام لین های مصرف کننده عمومی برق باید به صورت واضح مشخص شود: عنوان استفاده خاص، شدت جریان برق، ولتاژ، نوعیت، اتصال، محل وطول کیبل را برچسپ بزنند. در صورت جابجایی تجهیزات باید اسناد مربوطه بروزرسانی شود.

تجهیزات و کیبل ها

تجهیزات، وسایل جانبی همراه با کیبل ها در دیتاسنتر وتسهیلات مهم باید مطابق با ااستندرد (TIA 942) نصب شود تمام کیبل ها به صورت درست توسط Zip tie (بست کمربندی) بسته گردند.

کارمند دیتاسنتر مسئوول تمام معلومات و تجهیزات نصب شده در داخل دیتاسنتر هستند و از اجرا یا نصب وسایل در سایت های بیرونی باید آگاهی دا شته با شند. اگر قراردادی صلاحیت این را دا شته با شد که بعضی از تجهیزات را نصب نماید، باید توسط مدیر عمومی ارتباطات استراتیژیک ارزیابی گردد که آیا مطابق نیازمندی میباشد یا خیر؟ در جریان کار و ختم گزارش تمام کار های انجام شده توسط قراردادی به صورت کتبی ترتیب و به مرجع مربوطه ارائه گردد.

تمام کیبل ها باید به شکل درست و منظم در کیبل تری (جعبه کیبل) قرار بگیرد و کیبل های ارتباطی باید به صورت موازی نصب گردد.

تمام قراردادی های استخدام شده که در داخل دیتا سنتر کار می کنند اعم از برقی و افراد تخنیکی باید کار و وظایف محوله خویش را درهماهنگی و تفاهم با مدیریت عمومی ارتباطات استراتیژیک و دیتاسنتر تنظیم نمایند.

در ختم کار، تسلیم دهی تمام تجهیزات باید با هماهنگی با مدیران بخش مربوطه صورت گرفته تا از دریافت و سالم بودن، اطمینان حاصل گردد. بخش سفارش کننده تجهیزات، مسئوولیت اطلاع رسانی و قبولی تجهیزات را دارد.

پاکیزگی محیط دیتاسنتر

سطح فوقانی وتحتانی کف کاذب (Rise Floor) و تجهیزات ملحقه آن حداقل سالی یک بار پاک کاری گردد. این پاک کاری شامل پاک نمودن تمام لین های زیر کف کاذب، کاشی های کف کاذب وگرد و آلودگی نشسته در قسمت های داخلی وبیرونی رک های (الماری های) سرور میباشد. این کار باید توسط شخصی مسلکی صورت گیرد.

قسمت های داخلی دیتاسنتر باید به طور برنامه ریزی شده حداقل درماه یک بار پاک کاری گردد. شخص پاک کننده باید در زمینه آموزش دیده باشد.

وظایف و مکلفیت کارمندان

آوردن، صرف ونوشیدن هرنوع غذا ونوشیدنی در داخل دیتاسنتر جداً ممنوع است.

کارمندان مجاز نباید به تجهیزات ورک های که متعلق به دیگران است تماس داشته باشند.

اگر کدام رک بین دو بخش شریک باشد درصورت ضرورت به عیارسازی سیستم های موجود در بین آن رک، بعد از استیذان مدیر دیتاسنتر صورت گیرد.

کارمندان مجاز به ورود و دخول به دیتاسنتر مکلف به خانه پوری فورم ضمیمه نمبر 1 میباشد.

نظارت تصویری دوربین های مدار بسته (CCTV)

دوربین های مدار بسته (CCTV) به خاطرحفاظت از ساختمانها واموال، نظارت بر دسترسی به سیستم ها میباشد. شرایط بکارگیری و استفاده از دوربین های مدار بسته قرار ذیل است:

- بخش های اساسی شبکه ناک، دیتاسنتر و اطاق سرورهای ساحوی باید دارای دوربین های مدار بسته (CCTV) باشد و دوربین ها به شکل مناسب آن نصب گردد.
- هرگونه درخواست دسترسی به معلوماتی ذخیره شده توسط دوربین های مدار بسته باید به صورت کتبی به ریاست عمومی مخابره و تکنالوژی معلوماتی یا معاونین پیشنهاد گردد وبعد از دریافت هدایت شخص ریاست عمومی مخابره و تکنالوژی معلوماتی یا معاونین، مدیریت ع ارتباطات استراتیژیک معلومات ذخیره شده را برای مرجع مطالبه کننده در مدیریت ع ارتباطات استراتیژیک به نمایش گذاشته وثبت دفتر مربوطه نمایند.
- ریاست عمومی مخابره و تکنالوژی معلوماتی میتواند با استفاده ازسیستم دوربین های مدار بسته (CCTV) از شعبات، دفاتر و پرسونل ریاست عمومی مخابره و تکنالوژی معلوماتی کنترول ونظارت نماید.
- کمره های امنیتی در ساحاتی که حریم خصوصی دارد (تشناب، اطاق تبدیلی لباس) نباید نصب گردد.
- هر شخصی که سبب دستکاری یا تخریب دوربین ها مدار بسته یا دستگاهای مرتبط آن گردد باید به مدیریت مربوطه بخش امنیتی گزارش داده شود.
- تمام تصاویر ضبط شده (DVR) تا مدت 60 روز ذخیره خواهند شد و بعد از آن به صورت خودکار برروی آن تصاویر دیگر ضبط خواهد شد. مگر اینکه به عنوان بخشی از تحقیقات جنایی مورد استفاده قرار بگیرد.
- تمام ویدیوهای ضبط شده باید درمکان مطمئن و امن نگهداری گردد افراد مسئوول اجازه دسترسی داشده باشند.
- در صورت خرابی سخت افزار دوربین های مدار بسته یا مشکل در ضبط کردن تصاویر، فرد مسئوول باید در اسرع وقت به مدیریت مربوطه گزارش داده و درصورت نیاز درخواست اکمال آن را به بخش مربوطه ارسال نماید.
- راپور هفته وار از فعال بودن کمره های امنیتی توسط شخص مسئوول به مدیریت عمومی ارتباطات استراتیژیک ارسال گردد.
- در صورت بروز هرنوع مشکل در بخش کمره های امنیتی راپور آن به اسرع وقت ترتیب و به مدیریت کمره ها ارسال گردد.

امنیت شبکه

زیربنای تکنالوژی معلوماتی وزارت اموراخله بروی وسایل شبکه، سرورها وسایر خدمات مربوطه دیگر استوار است. تجهیزات شبکه ای در اجرای فعالیت های وزارت امور داخله نقش حیاتی داشته وروی تداوم کار وزارت تاثیر مستقیم دارد. تأمین و فراهم آوری یک شبکه قابل اعتبار از اهداف اصلی مدیریت عمومی شبکه بوده و تمامیت و امنیت این شبکه از کار های اصلی این مدیریت است. بیشتری از تجهیزات مربوط به شبکه را دراین جا تحت پوشش قرار داده وپالیسی های مشخص برای استفاده، فعالیت ونظارت وسایل شبکه تعیین میکند.

هدف ازطرح این طرزالعمل تعریف نمودن قوانین ومقررات غرض گزینش، تنظیم، محافظت، تأمین، عیارسازی، نظارت وحفظ ومراقبت وسایل مربوط به شبکه و ساختن بک آپ از عیارسازی وسیستم عامل ویندوز و بازگردان (Restore) آن در زمان نیاز به وسایل میباشد.

وسایل شبکه تجهیزات کلیدی هستند که سرورها و کلاینت ها(کمپیوترها) به خاطر تأمین ارتباطات از آن استفاده میکنند که قرار ذیل میباشند:

کیبل ها

انواع کیبل های که مورد استفاده قرار میگیرد قرار ذیل میباشد.

- کیبل های UTP Cat 5e(پوش دار) یا بالاتر از آن به خاطر وصل نمودن وسایل شبکه و آی پی کمره ها استفاده میگردد.
- کیبل های فایبر نوری یک مود، چندین مود.
- کیبل کوکسیل، ویرلس و تجهیزات ستلایت.

لین دوانی (wiring)

- تمامی لین دوانی باید علامت گذاری(Labeling) گردد.
- پورت های شبکه که مورد استفاده قرار نمی گیرد غیر فعال گردد.
- تمام کیبل های شبکه باید به شکل دوامدار شناسایی شده وبرای مراجعات بعدی ثبت گردد.
- کاربران نباید بالای کیبل های شبکه کدام چیزی را بگذارند.
- درصورت امکان بین بعضی وسایل بسیار مهم مانند سویچ ها وفایروال ها از کیبل ذخیره (Redundancy) به خاطر تأمین بهتر ارتباطات استفاده گردد.
- وال جک ها باید Cat5e یا بالاترآنرا حمایت نموده و بصورت ااستندرد A و B بوده وعلامت گذاری (Labeling) شوند.
- تمامی پچ پنل هایی (Patch Panel) که در شبکه موجود هستند باید به صورت مدل جدید بوده وختم هرکیبل به پچ پنل باید به صورت درست علامت گذاری شود.
- همه پچ پنل ها(Patch Panel) باید به صورت فیزیکی امن بوده و کیبل های Cat5e یا مدل بالاتر را حمایت کند.

سویچ ها:

سویچ ها تجهیزات کلیدی شبکه وزارت بوده و تمام سویچ هایی که در شبکه استفاده میگردد باید قرار ذیل باشد:

- سویچ ها باید مدل روز باشد. یعنی مشخصات آنها باید ضروریات فعلی و بعدی را مرفوع سازد.
- سویچ ها باید پروتوکول (Spanning Tree) را حمایت نمایند و از به جود آمدن لوپ (Loop) جلوگیری کنند.
- به مقصد مدیریت نمودن سویچ ها باید به Management VLAN آی پی آدرس جایگزین شود.
- آی پی Management VLAN باید فقط توسط مدیر شبکه قابل دسترس باشد.
- به منظور نظارت وراپوردهی در سویچ ها باید SNMPv3 فعال گردد.
- سویچ ها باید به صورت فیزیکی داخل رک ها امن بوده و قفل گردد، وکلید ها باید داخل جعبه محفوظ نگهداری گردد.

- رک هایی که سویچ ها در داخل آن نگهداری میگردد باید مجهز به پکه بوده و همیشه سرد باشد.
- تمام سویچ ها باید به یو پی اس وصل باشد تا از خاموش شدن یک دفعه ای آن جلوگیری گردد.
- اگر سویچ ها دارای پورت کنسول باشد باید توسط رمز عبوری محافظت گردد.
- Telnet باید در داخل سویچ ها غیر فعال گردد و SSH ورژن 2 باید استفاده گردد وتوسط رمز عبوری محافظت گردد.
- دسترسی از طریق HTTP میتواند صورت گرفته ولی باید با رمز عبوری محافظت گردیده باشد.
- لینک های ترنک شده باید ازیک سویچ به سویچ دیگر توسط گیگابیت ایترنت (Gigabit Ethernet) پورت وصل گردیده درصورت نداشتن پورت مذکور از پورت های فست ایترنت (Fast Ethernet) استفاده صورت گیرد.
- کیبل استفاده شده به خاطر ترنکینگ باید فایبر باشد در صورت نبود فایبر باید از Cat 6 یا بالاتر استفاده گردد.
- فایل های عیارسازی سویچ باید به داخل بک آپ سرور، بک آپ گرفته شود یا میتوان به داخل یک هارد دیسک بیرونی بک آپ گرفت و درجای محفوظ نگهداری گردد.
- سیستم عامل سویچ ها باید به اسرع وقت آپگرد (Upgrade) گردد وسیستم عامل جدید پیش از کار باید چک گردد.
- وقتی سویچ ها سفارش وخریداری میگردد باید خدمات بعد از فروش در آن ذکر گردد.

روتر

روترهم یکی از وسایل هستوی شبکه وزارت داخله بوده وهر روتر که در شبکه وزارت داخله وصل میگردد باید از قوانین ذیل پیروی کند.

- روتر باید به مدل روز باشد.
- در خرید روتر باید موارد ذیل مد نظر گرفته شود:
  - سایز شبکه که روتر برای آن خریداری میگردد.
  - انواع انترفیس هایی که مورد ضرورت است.
  - مقدار رم (RAM) مورد نیاز باید سنجش شود.
  - مقدار حافظه فلش مورد نیازباید سنجش شود.
  - مقدار NVRAM مورد نیاز باید سنجش گردد.
  - ورژن سیستم عامل یا (IOS) باید در نظر گرفته شود.
  - پشتیبانی یا حمایت برای خدمات نظر گرفته شود.
- نام کاربر ورمز عبوری ابتدایی باید تغییر کند.
- رمز عبوری که استفاده میگردد باید مغلق بوده یعنی متشکل ازاعداد وحروف بزرگ وکوچک باشد.
- User Exec مود و Privileged Exec مود باید با رمز عبوری محافظت گردد.
- تلنت (Telnet) به روتر باید غیر فعال گردد. میتوان از SSHv2 استفاده نمود و اگر روتر آنرا حمایت کرده بتواند باید با رمز عبوری محافظت شده باشد.
- تمام روتر ها باید ازطریق AAA سرور (Cisco Secure ACS) مورد دسترس قرار گیرد.
- سیستم عامل های که مبنی بر فایروال بوده باید در روتر هایی که در حاشیه یا مقابل به انترنت بوده قرار گرفته وفعال گردد.

- روتر باید از طریق آی پی آدرس های مشخص شده مجاز مورد دسترس قرار گرفته که در لیست به آن اجازه ورود به روتر را داده شده باشد.
- هیچ شخصی بجز مدیر شبکه حق ورود به روتر را از طریقSSH ندارد. در صورت مشاهده هرنوع حمله یا سواستفاده که از طریق شبکه داخلی صورت میگیرد باید به تیم امنیت شبکه گزارش داده شود.
- تمام پورت های (Interface) غیر ضروری باید غیر فعال گردد.
- پورت کنسول (Console) باید با رمز عبوری محافظت گردیده باشد.
- دسترسی فیزیکی به روتر باید فقط صرف به اشخاص مجاز محدود گردیده ونظر به نکات ذیل نگهداری گردد:
  - اگر روتر داخل اتاق مخصوص سرورها یا سویچ ها که مجهز به قفل باشد میتوان آنرا در داخل رک های باز قرار داد.
  - اگر روتر بیرون اتاق مخصوص روتر یا سویچ گذاشته باشد که در آنجا قفل برای دروازه نیست و دسترسی فیزیکی به روتر صورت گرفته میتواند پس آنرا باید در یک رک بسته که دارای پکه خنک کننده است قرار داده سپس قفل نمایید.
  - روتر باید به UPS وصل بوده در داخل رک قرار گیرد در صورت نبود جای برای UPS میتوان آنرا بیرون از رک قرار داد.
- در صورت عدم ضرورت روتر باید نکات ایمنی ذیل غیر فعال گردد.
  - سرور های کوچک برای TCP و UDP.
  - BOOTP (Bootstrap Protocol).
  - Finger Services.
  - HTTP.
  - CDP (Cisco Discover Protocol).
  - Auto – Loading.
  - خدمات غیر ضروری دیگر(Other Unnecessary Service).
  - Source Route.
- در قسمت پورت ها (Interface) باید نکات ذیل در نظر گرفته شود:
  - انترفیس های غیر قابل استفاده (Unused Interfaces).
  - توشیع مستقیم آی پی (IP directed-broadcast).
  - Proxy ARP.
  - ICMP unreachable.
  - IP Redirect.
  - IP Mask replies.
  - NTP Service.
  - SNMP unless it is required.
- روتینگ پروتوکول هایی که ضرروری نیست نباید فعال گردد مگر در صورتیکه ضرورت باشد باید پروتوکول هایی فعال گردد که آنها Authentication را حمایت نماید.
- مسیر های ثابت (Static Route) باید بر مبنای مسیر مقصد(Destination) در شبکه تعریف گردد.

فایروال

فایروال نیز هم یکی از وسایل مهم شبکه وزارت داخله بوده و هر فایروال که در شبکه وزارت داخله وصل میگردد باید از قوانین ذیل پیروی کند.

- فایروال باید به مدل روز باشد.
- وقتی یک فایروال خریداری میگردد باید موارد ذیل درنظر گرفته شود:
- سایز شبکه که فایروال برای آن خریداری میگردد.
- انواع انترفیس هایی که مورد ضرورت است.
- مقدار رم(RAM) مورد نیاز باید سنجش شود.
- مقدار حافظه فلش مورد نیازباید سنجش شود.
- مقدار NVRAM مورد نیاز باید سنجش گردد.
- ورژن سیستم عامل یا (IOS) باید درنظر گرفته شود.
- پشتیبانی یا سپورت برای خدمات نظر گرفته شود.
- نام کاربر ورمز عبوری اولیه باید تغییر یابد.
- رمز عبوریی که استفاده میگردد باید مغلق بوده یعنی متشکل ازاعداد و حروف بزرگ وکوچک باشد.
- User Exec مود و Privileged مود باید با رمز عبوری محافظت گردد.
- تلنت (Telnet) به فایروال باید غیر فعال گردد.
- میتوانیم از SSHv2 استفاده نموده اگر فایروال آنرا سپورت کرده بتواند، وباید با رمز عبوری محافظت شده باشد.
- تمام پورت های (Interface) غیر ضروری باید غیرفعال گردد.
- دسترسی فیزیکی به فایروال باید قطعا صرف به اشخاص مجاز محدود گردیده ونظر به نکات ذیل نگهداری گردد:
- اگر فایروال داخل اتاق مخصوص سرورها یا سویچ ها که مجهز به قفل باشد میتوان آنرا در داخل رک های باز قرار داد.
- اگر فایروال بیرون اتاق مخصوص روتر یا سویچ باشد دروازه آنجا باید قفل شده و در یک رک بسته که دارای پکه خنک کننده است قرار گرفته، قفل شود.
- فایروال باید به UPS وصل بوده در داخل رک قرار گیرد در صورت نبود جای برای UPS میتوان آنرا بیرون از رک قرار داد.
- در صورت عدم ضرورت باید نکات ذیل در فایروال غیر فعال گردد.
- سرور های کوچک برای TCP و UDP.
- BOOTP (Bootstrap Protocol).
- Finger Services.
- HTTP
- CDP (Cisco Discover Protocol).
- Auto – Loading.
- خدمات غیر ضروری دیگر(Other Unnecessary Services).

- Source Route
- در قسمت اینترفیس های باید نکات ذیل در نظر گرفته شود:
  - اینترفیس های غیر قابل استفاده(Unused Interfaces)
  - توشیع مستقیم آی پی (IP directed-broadcast)
  - Proxy ARP
  - ICMP unreachable
  - IP Redirect
  - IP Mask replies
  - NTP Service
  - SNMP unless it is required
- روتینگ پروتوکول هایی که ضرروری نیست نباید فعال گردد.
- مسیر های ثابت (Static Route) باید برمبنای مسیر مقصد (Destination) در شبکه تعریف گردد.
- اگر انترفیسDMZ استفاده گردیده باشد وسایلی که درساحه DMZ قرار میگیرند نباید کاملا مورد اعتماد وسایل که در شبکه داخلی قراردارند قرار گیرد.
- فقط سرویس هایی که به صورت عموم هستند باید به انترفیس DMZ قرار گیرند.
- سطح امنیتی برای انترفیس DMZ باید زیر 50 باشدو سطح امنیتی برای انترفیس های داخلی باید 100 باشد.
- سطح امنیتی برای انترفیس های خارجی باید 0 باشد.
- انترفیس Failover باید برای خدمات بسیار مهم و کلیدی استفاده گردد.
- برای خدماتی که داخل شبکه وجود دارد وضرورت است تا از انترفیس بیرونی به آن دسترسی پیدا شود باید عملیه NAT استفاده گردد. فقط پورت های ضروری خدماتی باید برای عبور و مرور از بیرون به داخل اجازه داده شود.
- فایل های عیار سازی فایروال باید بک آپ گرفته ودر سرور یا هارد دیسک، حافظه برای آن تخصیص داده شده و به صورت امن نگهداری گردد.
- در صورت ضرورت باید طریقه Content Filtering عیار سازی گردد.
- برای سایت های دسترسی از راه دور(Remote Site) باید VPN به خاطر وصل نمودن سایت ها از طریق اینترنت استفاده گردد.
- از لیست دسترسی (Access List) برای رد کردن ترافیک بر مبنای (Source IP, Destination IP Protocol, source Port, Destination Port TCP and UDP) استفاده و عیارسازی گردد.
- نوعیت ASA(فایروال) به وسعت شبکه ارتباط داشته و ویژگی های ASA(فایروال) نظر به ضرورت فعال گردد.
- تمام ترافیک که داخل یا بیرون میگردد باید از میان ASA(فایروال) عبور کند.
- یو آر ال (URL Filtering) باید در داخل ASA (فایروال) فعال گردد درصورتیکه امکانات دیگر URL filtering موجود نباشد.
- ارایه لیسنس ها(License) باید توسط شخص تعیین شده مورد مراقبت قرار گیرد.
- تمام ترافیک که ضروری میباشد باید از طریق DMZ به انترفیس داخلی اجازه داده شود.
- فایرفاکس (Failover) باید موجود باشد درصورت که این یکی از وسایل مرکزی باشد.

فصل دوم

امنیت سایبری برای کاربران

فراهم آوردن یک محیط عملیاتی مطمئین و محفوظ که وزارت امور داخله را در جریان فعالیت های روزمره و عملیات های مهم حمایت می کند یک امر فوق العاده مهم بوده که برای تهیه چنین محیط مساعد پروسه های خاصی تهیه و تدوین شده است. این پروسیجرها به اساس اهداف استراتیژیک امنیت سایبری و پروسیجر وزارت امور داخله بنا گردیده است که اهداف ذیل را شامل می شود:

- محافظت شبکه وزارت امور داخله از تهدیدات، تهدیدات ویروس و استفاده نارست از تجهزات.
- ایجاد یک چارچوب امنیتی برای دسترسی مناسب به منابع وخدمات معلوماتی.
- محافظت بر خلاف دسترسی غیر مجاز، استفاده یا شریک ساختن معلومات حساس که منجر به آسیب پذیری و سوء استفاده از شبکه وزارت امور داخله میگردد.
- محافظت دربرابر تهدیدات پیش بینی شده و خطرات امنیتی که متوجه معلومات طبقه بندی می باشد.
- مبارزه موثر علیه فساد وایجاد شفافیت در خدمات.
- حفظ ارتباط امن بین دوشخص وافشا نکردن اسناد محرم.
- توسعه واستفاده موثرازتمام تجهیزات تکنالوژی معلوماتی مانند کامپیوتر، پرینتر، (VoIP) وایپ و سایر دستگاه های شبکه.

ایجاد حساب (User Account) برای کاربران

کاربران شبکه وزارت اموردا‌خله باید منسوبین قواي پولیس ملی افغانستان یا مامورین ملکی وزارت اموردا‌خله باشند.

درصورتیکه درخواست کننده خارج ازتشکیل وزارت اموردا‌خله باشد به اساس سند رسمی و منظوري آمرین (قوماندانان) مربوطه شامل لیست کاربران میشوند.

فورم مشخص که برای ایجاد حساب کاربران شبکه ترتیب گردیده ازطرف مسئوول مخابره برای کاربر توزیع میگردد. کاربر بعد ازمطالعه وپذیرفتن شرایط مندرج، فورم مذکور را خانه پري و امضا نموده و بعد به آمرمخابره و تکنالوژی معلوماتی تسلیم مینماید.

آمرمخابره و تکنالوژی معلوماتی فورم ها راجمع آوري نموده و بعد از ملاحظه شد قوماندان یا آمرین مربوطه حساب کاربر را تایید و ترتیب مینماید.

اسم کاربر درتمام سطوح وزارت اموردا‌خله یکسان(واحد) بوده و برای سهولت از اوت لوک (Outlook) استفاده شود که برای دریافت معلومات مربوط از طریق اوت لوك حساب کاربر بشکل تخلص،اسم، رتبه، وظیفه جزوتام جزوتام مافوق ترتیب میگردد.

کاربران شبکه وزارت اموردا‌خله، به منظورمطالعه وفراگیري آموزشهای آنلاین، رفع خستگی، تفریح وآگاه شدن از وضعیت اخبارسایت های خبري و معلوماتی ملی و بین المللی فعال و مجاز را استفاده نموده میتوانند.

کاربران ازاشتراك در پروگرامهای غیرمجاز وچاپ عکس ها که به حیثیت و وقار وزارت اموردا‌خله صدمه میرساند و یا باعث زیان اقتصادي به اداره شود جداً جلوگیري نموده درغیرآن مورد بازپرس قانونی قرارمیگیرند.

بنابرملحوظات امنیتی، صلاحیت عموم کاربران ازشبکه وزارت اموردخله محدود بوده البته درصورت ارتقا وتوسعه قابلیت ها تفویض صلاحیت ها امکان پذیرمیباشد.

درصورت نیاز مبرم منسوبین برای دسترسی به یکی ازسایت های مشخص معلوماتی ویا اینکه درجریان اجرا ي وظیفه محوله به آن ضرورت محسوس گردد. دراین حالت سند رسمی با توضیح شهرت، وظیفه وسایت مورد ضرورت ازطرف مرجع وظیفه داري اش ترتیب وبعد ازمنظوري شخص ریاست عمومی مخابره و تکنالوژی معلوماتی برایش درسایت مورد نیاز صلاحیت دسترسی داده شده یک نقل آن به مسئوول سرور ارسال وباقی اسناد درمدیریت ارتباطات استراتیژیک معلوماتی نگهداري میشود.

هر منسوب چه افسر ویا قراردادي باشد بدون تکمیل فورم توافق نامه دسترسی صلاحیت دسترسی به شبکه وزارت اموردخله را ندارد. اصول متذکره درسطح تشکیلات ساحوي نیز قابل تطبیق میباشد.

استفاده درست

هدف از طرح و ترتیب پالیسی استفاده درست، ایجاد امنیت و مصئونیت اطلاعات برای محافظت کارمندان وزارت در برابر اعمال غیر قانونی و مخرب توسط افراد که به صورت خواسته یا ناخواسته طرح گردیده است.

سیستم انترنت، انترانت واکسترنت (داخلی وبیرونی) بشمول تجهیزات کامپیوتری، سافت ویر، سیستم عملیاتی، وسایل ذخیره معلومات، حساب های شبکه ای متشکل از برنامه های ایمیل، بروزینگ و مانند آن همه منحیث دارایی های وزارت امور داخله محسوب میگردد.

این پالیسی بر تمامی منسوبین وزارت امور داخله، کارمندان قراردادی ومشاورین قابل تطبیق است وتمامی تجهیزات را که متعلق به وزارت ویا تحت نظر آن باشد را مورد پوشش قرار میدهد.

استفاده درست شامل نکات ذیل میباشد:

- استفاده عمومی و مالکیت
- اطلاعات امنیتی و اختصاصی
- استفاده نادرست وغیر قابل قبول
- فعالیت های مربوط به سیستم شبکه
- رمز عبوری
- فعالیت های مربوط به ایمیل وارتباطات
- رمز گزاری یا انکریپشن

استفاده عمومی و مالکیت

برای استفاده درست از امکانات فراهم شده در بخش مخابره و کمپیوتر نکات ذیل مد نظر گرفته شود:

- کارمندان و منسوبین به تمام ویب سایت های دولتی که با پسوند gov.af است، دسترسی خواهند داشت.
- منسوبین به تمام ویب سایت های داخلی که با پسوند af. است دسترسی خواهند داشت.

- منسوبین به تمام ویب سایت های داخلی و خارجی که به نحوی با وزارت امور داخله در ارتباط هستند، دسترسی خواهند داشت.
- کارمندان صرف از کمپیوتر، حساب کمپیوتر وفایل های کمپیوتری که حق دسترسی مجاز به آنرا دارند استفاده کرده میتوانند.
- کارمندان نباید از حساب کمپیوتر کسی دیگر استفاده کنند و یا کوشش نمایند تا رمز عبوری کسی دیگر را بگیرند یا در صدد پیدا کردن آن باشد.
- هر کاربر به تنهایی مسئوول استفاده درست از تمام منابع که برایش اختصاص داده شده بشمول کمپیوتر، آدرس شبکه و پورت، نرم افزار وسخت افزار میباشد بنابراین شما پاسخگو به وزارت بوده و نباید اشخاص غیر مجاز از آدرس شما به شبکه وصل گردند.
- کاربران نباید کوشش کنند که به بخش های محرمانه شبکه، سیستم عامل، نرم افزار و یا برنامه های کاربردی اداری دسترسی داشته باشند.
- کاربران نباید از منابع شبکه و وسایل در رابطه به اجرا نمودن پروگرام ها، نرم افزار و عملیه های دیگر که سبب مختل شدن کمپیوتر، کاربران شبکه، آسیب رسانیدن، کاهش آمدن در روند کار بخش نرم آفزار و سخت آفزار استفاده گردد.
- در شبکه وزارت و سیستم های کمپیوتری نباید از ابزارهای که به خاطر دسترسی امنیتی و یا حملات کمپیوتری و شبکه ایی مانند Password Crackers، Vulnerability Scanners، Network Sniffers استفاده گردد، مگر آنکه برای استفاده از آن صلاحیت قانونی داشته باشد.
- از تمامی کاربران شبکه و منابع کمپیوتری توقع میرود تا به حریم وحقوق شخصی دیگران احترام بگذارند.
- بدون اجازه مکتوبی، دسترسی یا گرفتن کاپی ایمیل، دیتا، برنامه و دیگر فایل های کاربران مجاز نمیباشد.

درحالیکه مدیریت شبکه وزارت یک حد معین محدودیت را برای کارمندان ارائه میکند کاربران باید بدانند که معلوماتی را که داخل سیستم مینمایند جز دارایی و ملکیت وزارت پنداشته میشود.

مدیریت شبکه پیشنهاد میکند که تمامی معلوماتی که کاربر ها آنرا حساس و یا آسیب پذیر می پندارند باید رمز گزاری (انکریپت) گردد. مسئولین مدیریت شبکه میتوانند که کارمندان را راجع به محرم ساختن اطلاعات آموزش دهند.

به هدف تأمین مصئونیت وحفظ وتداوم شبکه، مسئولین مدیریت شبکه وزرات میتوانند طبق پالیسی بازرسی از سیستم ها، شبکه ها و تجهیزات وترافیک اطلاعات در سیستم های وزارت را مورد نظارت و ارزیابی قرار دهند.

مسئوولین مدیریت شبکه باید به طور متواتر از سیستم ها و شبکه ها به منظورتطابق و رعایت پالیسی نظارت و بازرسی نمایند.

تجهیزات تکنالوژی معلوماتی که به کاربران تسلیم میگردد منحیث دارایی شخصی محسوب نمیشود صرفا تنها حق استفاده از این وسایل را دارا میباشند.

تمام کمپیوتر های وزارت اموراخله باید دارای سیستم عامل بروز شده (Update) مانند ویندوز 8 یا 10 را داشته باشند.

در هرکمپیوتر آنتی ویروس باید نصب گردیده باشد و به شکل منظم و دوامدار کمپیوترمذکور باید اسکن و بروزرسانی گردد.

حساب مدیریتی(Administrator) باید همراه کاربر شریک نگردد صرف کارمندان بخش شبکه باید بتوانند به حساب مدیریتی دسترسی داشته باشند.

تمامی برنامه های غیر ضروری و تثبیت ناشده باید از کمپیوترهای وزارت امور داخله حذف گردیده و مسئولین شبکه ناک وزارت امور داخله میتوانند بصورت ناگهانی کمپیوترها را مورد بازرسی قرار دهند.

هر کمپیوتر به خاطر دسترسی به انترنت و شبکه باید شامل دومین(Domain) گردد و گروپ پالیسی بالای آن تطبیق گردد. نظر به هر دلیلی اگر کمپیوتری شامل دومین وزارت امور داخله نباشد نباید به شبکه انترنت و انترانت(داخلی) وزارت امور داخله وصل گردد.

هیچ کمپیوتری صلاحیت وصل شدن به شبکه وزارت امور داخله قبل از اخذ اجازه مکتوبی بخش ریاست عمومی مخابره و تکنالوژی معلوماتی را ندارد.

هر کمپیوتر ازطریق سرور(دی اچ سی پی) آی پی آدرس را اخذ نموده در صورت بروز هر نوع مشکل بخش آی تی را اطلاع دهند.

پرینتر شبکه صرف از طریق مدیریت عمومی ارتباطات استراتیژیک برای مدیریت های دیگر نصب میگردد و باید دارای یک نام مشخص و آی پی آدرس ریزرف شده باشد. هنگام برقراری ارتباط با دیگران با استفاده از سیستم های کمپیوتری باید بصورت ادبی و حرفه ای باشید. استفاده از وسایل کمپیوتری به خاطر تهمت و یا اذیت دیگران اجازه نیست و کسانی که آنرا نقض میکنند همرایشان به صورت قانونی برخورد صورت خواهد گرفت.

اطلاعات امنیتی اختصاصی

معلومات محرم باید سری نگهداشته شده یا رمز گزاری گردد و تدابیر لازمه برای جلوگیری از استفاده و دسترسی غیر مجاز به این اطلاعات را اتخاذ نمایند.

کاربران رمز عبوری(رمز عبوری) را مصئون نگهداشته و با دیگران شریک نسازند. کاربران مجاز مسئوولیت حفظ رمز عبوری ها و حساب های شان را دارند رمز عبوری های کاربر (User Account Password)باید در هر دو ماه تبدیل گردد.

تمامی کمپیوترها، لپ تاب ها وسیستم های کمپیوتری باید با رمز عبوری محافظت گردند و به شکل اتوماتیک در صورت عدم استفاده باید کمتر ازچند دقیقه قفل گردد همچنان زمانی که کاربرها کمپیوتر خویش را ترک مینمایند باید سیستم خویش را قفل نمایند.

صرف از ویب سایت های مجاز برای امور کاری روزمره استفاده گردد وتمامی سایت های غیر مجاز که به حیطه کاری وزارت امور داخله مرتبط نمی باشد باید مسدود گردد.

کارمندان باید در موقع باز کردن ضمیمه های ایمیل از احتیاط تمام استفاده نمایند چون خطر موجودیت ویروس، تروجن وغیره نرم افزارهای خطرناک میباشد.

استفاده نادرست وغیر قابل قبول

در هیچ حالات وشرایط کارمندان وزارت حین استفاده از منابع وزارت حق ندارند که در فعالیت های که طبق قوانین نافذه کشور منع قرار داده شده است دخیل باشند.

فعالیت های ممنوع در سیستم و شبکه

فعالیت های ذیل بدون هیچ گونه استثنا جداً ممنوع قرار داده شده است:

- نصب هر گونه نرم افزار که وزارت یا کاربر دیگر برای استفاده از آن مجوز فعال ندارند جدا ممنوع است.
- معرفی برنامه یا پروگرام های غیر مجاز در شبکه یا سرور(ویروس، وارم، ترجان هارس، ایمیل سپم وغیره)
- افشا کردن رمز عبوری برای دیگران و یا اجازه برای دیگران غرض استفاده از حساب.
- پیشنهاد و ارائه فریب آمیز هرگونه وسایل اشیا و خدمات که از آدرس وزارت نشئات میگیرد.
- ترتیب ضمانت خط مستقیم یا غیر مستقیم الی اینکه این عمل جز لایحه وظایف باشد.
- اجازه تخلفات امنیتی یا اختلال در سیستم و شبکه، تخلفات امنیتی بشمول دسترسی به معلومات که کارمند در واقع دریافت کننده آن نیست و یا داخل شدن به سرور یا حساب که کارمند رسما اجازه آنرا ندارد جز اینکه این کار در لایحه وظایف کارمند درج باشد..
- هر نوع اسکن کردن شبکه و یا اسکن امنیتی بدون اطلاعیه قبلی جدا ممنوع می باشد.
- تلاش برای جلوگیری از تثبیت هویت کاربر، امنیت کمپیوترهای وصل شده، شبکه وحساب.
- استفاده ازهر پروگرام، سکریپت، کماند و یا ارسال پیام به نحوه که هدف آن مداخله و یا غیر فعال ساختن برنامه کاربر از هر طریق ممکن چه از محل کار و یا از طریق انترنت باشد.
- ارائه معلومات یا فهرست کارمندان وزارت به بیرون از وزارت به استثناء اینکه شامل پروسه رسمی باشد.
- تغییر، عیار سازی مجدد نرم افزار و سخت افزار کمپیوتر یا شبکه های وزارت بدون اجازه قبلی مدیریت شبکه.
- عیار سازی وسایل و ارائه خدمات آی تی جز اینکه مسئوولین سیستم آنرا اجازه داده باشند.
- وصل کردن وسایل خارجی به کمپیوتر یا شبکه وزارت مانند فلش دیسک، اکسترنال هارددیسک، فلاپی دیسک، ام پی 3 پلیر، ای پاد وسایر وسایل حفظ و انتقال معلومات، جز اینکه اجازه قبلی در مورد آن اخذ شده باشد.
- شریک ساختن یک فایل، فولدر ویا سایر منابع شبکه ای بدون اطلاع اشخاص ذیصلاح.
- تغییر وجایگزینی سخت افزار کامپیوتر بدون اجازه مسولین سیستم شبکه وزارت امور داخله.
- ذخیره ونگهداری معلومات شخصی (عکس، فایل، موزیک، فیلم و غیره) که وزارت در صورت مفقود شدن این اطلاعات شخصی مسئولیت ندارد.

پسورد یا رمز عبوری

رمز عبوری جز مهم از آمنیت ومصئونیت حساب های کاربران و سیستم های معلوماتی است. رمز عبوری به مثابه خط مقدم درحفاظت از حساب های کاربر می باشد.استفاده از رمز عبوری های آسان یا ضعیف میتواند تمامی شبکه وزارت را در خطر بیندازد. بنابراین تمامی کارمندان وزارت مسئولیت دارند تا از تدابیر لازمه طبق اصول ذیل برای انتخاب وحفاظت از رمز عبوری

های شان استفاده کنند. هدف از این طرزالعمل ارائه رمز عبوری قوی و تهیه یک رهنمود برای حفاظت از رمز عبوریها میباشد. پالیسی رمز عبوری بالای تمام کاربرهای وزارت امور داخله که به منابع شبکه (ایمیل، ورود به کمپیوتر، ویا ورود به دیگر سیستم های داخلی) دسترسی دارند تطبیق میگردد.

- تمامی رمز عبوری سیستم ها(سرور، سویچ، روتر و غیره) باید حداقل درهر 9ماه تبدیل گردد.
- تمامی رمز عبوری های کاربران یا کاربرها (ایمیل، انترنت، کمپیوتر دسکتاپ و غیره) حداقل باید هر 60 روز تغییر داده شود. ورمز عبوری های مربوط به مدیران سیستم های شبکه باید هر 30 روز بعد تغییر داده وباید 15 حرف به صورت مغلق باشد. که مغلق بودن عبارت از حروف بزرگ وکوچک وعلایم وشماره باشد.
- تمامی رمز عبوری های کاربران یا سیستم باید مطابق به رهنمود ذیل تنظیم گردند.
- از حروف کوچک و بزرگ انگلیسی استفاده شود که دارای ارقام و علامات تحریری و حروف نیز باشد.
- دارای حداقل 10 حروف متفاوت و یا مانند یک عبارت نوشته شود.
- هیچگاه رمز عبوری تانرا از طریق تلیفون به کسی نگوید ویا از طریق ایمیل به کسی روان نکنید.
- در صورت داخل نمودن رمز عبوری به سیستم بعد از 7 بار حساب تان قفل گردیده و به همکاری تیم حمایوی بعد از اطلاع دهی پس برایتان باز میگردد.
- از رمز عبوری تکراری جلوگیری صورت گیرد مگر اینکه 5 بار رمز عبوری مختلف استفاده گردیده باشد.
- در مورد رمز عبوری تان در مقابل دیگران حتی آمرتان صحبت نکنید وهیچگاه آنرا در فورمه ها یا پرسشنامه های امنیتی نوشته نکنید.
- هیچگاهی از دستورهای مانند " رمز عبوری را به خاطر داشته باشید " که در کمپیوتر برایتان پیشنهاد میگردد استفاده نکنید.
- رمز عبوری تان را هیچگاهی در جایی نوشته نکنید و آنرا در دفتر نگهداری نکنید.
- هرگاه یک حساب یا رمز عبوری مورد شک قرارگرفته باشد باید دیپارتمنت تکنالوژی معلوماتی را از موضوع آگاه ساخته و تمامی رمز عبوریها باید تغییر داده شوند.

مصونیت سرورها

بمنظورجلوگیري ازخطرات وآسیب ها، وسایل موثرمانند فایروال ها، انتی ویروس ها وغیره نرم افزار های محافظوي نصب وطوردایم فعال نگهداشته شوند.

- دخول به سایت های غیر مجاز باید توسط یک پیام(وارنینگ) داده شود مانند: دسترسی تان به سایت مطلوب مسترد است.
- تمام پالیسی ها بشکل گروپ پالیسی ازطریق سرورهای مرکز عملیات شبکه طرح وتطبیق میشود.
- یک کاپی اسناد دسترسی به معلومات، سایت ها ویا محدود ساختن اختیارات عموم وسایل شبکه بشمول تیلیفون های وایپ درنزد مدیریت سرورها وکاپی دیگر اسناد درمدیریت شبکه و تکنالوژی حفا ظت می گردد.

- در جریان ویدیو کنفرانس ها تشریح پلان های امنیتی و سایرجلسات کوشش صورت گیرد که کدام شخص، با استفاده از وسایل اطلاعاتی مانند کمره های مخفی، تیلیفون های کمره دار و آلات ثبت صدا موضوع را افشا و نشر نکند.

دسترسی از راه دور به کمپیوتر(Remote Access)

دسترسی از راه دور (Remote Access) به کمپیوتر های شبکه وزارت اموراخله به صورت کلی مسدود میباشد وهیچ نوع صلاحیت دسترسی برای کاربران داده نمیشود. صرف در بعضی موارد حل مشکلات مسولین شبکه (مدیر شبکه یا مدیرسیستم) میتواند از دسترسی از راه دور استفاده نماید.

وصل نمودن کمپیوتر کاربر بدون اجازه کتبی (فورم توافق نامه کاربر) به شبکه مجاز نیست. نصب هیچ نوع سافت ویرهای دسترسی از راه دور (تیم ویور یا ریموت اسیستنت) مجاز نیست. دسترسی از راه دور توسط این چنین برنامه تهدید امنیتی برای کل شبکه می باشد.

دسترسی از طریق VPN

اجازه دسترسی از طریق VPN(شبکه شخصی مجازی) به شبکه وزارت امور داخله مجاز نبوده مگر اینکه از مقام وزارت احکام قاطع داشته باشند با وجود آن هم باید نکات ذیل را مراعات نمایند.

- فورم توافق نامه کاربر ضمیمه 2 را تکمیل نمایند.
- فورم دسترسی VPN ضمیمه 7 را تکمیل نمایند.
- کمپیوتر شخصی یا شرکت باید دارای ویندوز آپدیت و لیسانس بوده آنتی ویروس فعال و آپدیت داشته باشد.
- در صورتیکه آنتی ویروس کمودو(Commodo) باشد بهتر است.
- کمپیوتر در دفعه اول باید توسط تیم حمایوی شبکه ناک اسکن گردیده و برنامه های اضافی و غیر لیسانس از کمپیوتر متذکره پاگ گردد.
- دسترسی از طریق VPN صرف باید به سرورهای متذکره شان باشد.

ایمیل و فعالیت های ارتباطات

از انجایکه درتمام ادارات به خاطرتبادله معلومات وارتباطات ازایمیل الکترونیکی استفاده میگردد. استفاده نادرست از ایمیل عواقب خطرناک مانند ازبین رفتن حریم خصوصی، خطرات امنیتی وغیره صورت میگیرد اهمیت این موضوع سبب گردیده تا کاربران طریقه درست استفاده از ایمیل را درنظر داشته باشند.

تمامی ایمیل هایی که از طریق شبکه وزارت داخله تبادله میگردد ازجمله دارایی وزارت امور داخله میباشد. ایمیل های شما مورد نظارت قرار میگیرد درصورت استفاده نادرست از ایمیل وزارت اموراخله برخورد قانونی صورت میگیرد. از ایمیل به عنوان یک ابزار موثر وقانونی استفاده گردد نه برای استفاده شخصی.

استفاده از سیستم ایمیل وزارت امور داخله برای هرچیزی غیر ازاهداف قانونی ممنوع است. بنابراین، ارسال ایمیل شخصی، نامه های زنجیره ای، نامه های ناخواسته(Junk Email) وجوک ها ممنوع است.

درهنگام تبادله اطلاعات از طریق ایمیل وزارت امور داخله باید نکات ذیل درنظر گرفته شود.

- استفاده غیر مجازویا جعل کردن معلومات مندرج ایمیل ممنوع میباشد.
- ارسال ایمیل آدرس رسمی به آدرس مرجع غیر رسمی و صفحات اجتماعی ممنوع میباشد.
- استفاده از ایمیل آدرس اداره صرف درموضوعات و امور رسمی وزارت امور داخله مجاز بوده، در صورت استفاده غیر مجاز مسؤلیت بعدی متوجه شخص کاربر میباشد.
- در هنگام ارسال ودریافت معلومات حساس یا مهم باید بسیار محتاط بوده در صورت بروز هر گونه شک باید مدیر امنیت سایبری ارتباطات استراتیژیک را در جریان بگذارید.
- انتقال وارسال خودکار ایمیل های وزارت امور داخله به سیستم ایمیل آدرس ثالث ممنوع است. پیامهای شخصی که بین افراد توسط کاربر تبادله میگردد نباید حاوی اطلاعات وزارت امور داخله باشد.
- اگر شما پیام های مکرر، ناخوشایند، آزاردهنده و تهدید آمیز ازطریق ایمیل آدرس وزارت امور داخله دریافت میکنید موضوع را بلافاصله به مدیرتیم امنیت سایبری یا مسوؤلین تکنالوژی معلوماتی اطلاع دهید تا در اسرع وقت ردیابی گردد.
- درهنگام ارسال یا انتقال ایمیل باید تمام حروف ایمیل آدرس شخص دریافت کننده به صورت درست ودقیق بررسی گردد.
- دسترسی و ورود به ایمیل آدرس وزارت امور داخله از طریق هر نوع مرورگر(Browser) بیرونی جدا ممنوع است.

استفاده از وسایل جانبی وانترنت(Removal Media)

وسایل جانبی منبع شناخته شده انتقال ویروس ومورد هدف قرار گرفتن معلومات حساس در ادارات میباشد. به خاطر جلوگیری از خطر احتمالی در معرض قرارگرفتن معلومات مهم وزارت امور داخله ومصاب شدن به ویروس های گوناگون استفاده از وسایل جانبی (انواع یو اس بی، هارد دیسک بیرونی، سی دی، فلاپی دیسک،...) منع قرارداده شده است. به منظورانتقال ودریافت معلومات داخلی باید از پوشه های شریک شده (Share Folder) درهر اداره به صورت مستقل استفاده گردد. در صورت ضرورت اشد استفاده وسایل جانبی از قبیل (فلش، سی دی و غیره) باید تعهد از اداره مربوطه گرفته شود تا در صورت بروز هرنوع مشکلات وحملات سایبری جوابگوی باشند.

نصب هر نوع برنامه یا پروگرام از طریق وسایل جانبی در کمپیوتر های وزرات امور داخله ممنوع است.

در صورت که ضرورت مبرم به استفاده از وسایل جانبی در ادارات مربوط وزارت امور داخله محسوس گردد به اساس مطالبه یا تقاضای اداره نیازمند واحکام ریاست عمومی مخابره و تکنالوژی معلوماتی اجازه استفاده از وسایل جانبی داده میشود.

میعاد دسترسی به وسایل جانبی 6 ماه بوده و در صورت ضرورت مبرم بعد از ارایه پیشنهاد و تکمیل نمودن فورم دسترسی به وسایل جانبی از طرف اداره نیازمند برای 6 ماه دیگر تمدید میگردد (ضمیمه 3).

انترنت و شرایط استفاده از آن

استفاده ازانترنت صرف برای مقاصد اداری ووظایف رسمی میباشد. این طرزالعمل به صورت یکسان بالای تمام کاربرهای وزارت امور داخله اعم از کارمندان ملکی ونظامی قابل تطبیق میباشد. دسترسی به انترنت شبکه وزارت اموردداخله به مقاصد تبادله اطلاعات ودریافت معلوماتی مورد نیاز ادارات میباشد.

- اساسی ترین استفاده از انترنت توانایی دسترسی وتبادله فایل به صورت آسان وسریع میباشد که بخش تکنالوژی معلوماتی وزارت اموردداخله این سهولت رابرای کاربرهای وزارت امور داخله فراهم میسازد. بمنظور مقاصد امنیتی وحفاظتی، مسئوولین شبکه ناک وزارت امور داخله صلاحیت بررسی و کنترول از کارهای هر کاربر، استفاده از شبکه وخدمات وزارت امور داخله را دارند.

- استفاده از هرنوع سافت ویرهایی که سایت های مسدود شده از طرف وزارت امور داخله را بازنماید ممنوع می باشد.
- مدیریت ارتباطات استراتیژیک صلاحیت تعیین میزان استفاده و محدود ساختن انترنت (Bandwidth) آن عده از کاربرهای وزارت امور داخله که در استفاده از انترنت زیاده روی می نماید را دارد.
- هر نوع استفاده نادرست از انترنت (شریک ساختن آی پی ادرس از طریق کمپیوتریا اکسس پاینت)ممنوع میباشد.

مکلفیت ها وهدایات مندرج که در بخش " استفاده درست" کاربر از آن تذکر به عمل آمده در بخش استفاده از انترنت نیز قابل رعایت بوده ودرصورت تخلف از موارد فوق کاربر متخلف مسدود (بلاک) میگردد. به خاطر دوباره فعال ساختن آن باید فورم توافق نامه کاربر (ضمیمه 2) از طرف اداره نیازمند را با ذکر خلاف ورزی از طرزالعمل را تکمیل نموده وطی مراحل نماید.

دسترسی کامل به انترنت (Full Access)

دسترسی به شبکه واستفاده از منابع شبکه وزارت امور داخله صرف برای اجرا کارهای رسمی میباشد. به منظور تأمین امنیت شبکه وزارت امور داخله هر نوع دسترسی به سایت های اجتماعی (فیسبوک، یوتیوب، تویتر، سرگرمی و غیره) وآنعده سایت هایی که به اساس پالیسی های امنیتی داخلی شبکه (NOC) منع قرارداده شده مجاز نبوده و صرف در صورت موجودیت ضرورت مبرم و بعد از طی مراحل فورم دسترسی کامل(ضمیه 4) به استثنای فیسبوک (Facebook) اجازه دسترسی به آن داده میشود.

بلوکود

دستگاه بلوکود به خاطر دسترسی امن وسریع کاربرها به انترنت میباشد، دستگاه بلوکود سهولت های از قبیل دسترسی به منابع شبکه، محافظت درمقابل تهدیدات صفحات انترنتی وغیره را فراهم میسازد. دستگاه بلوکود به مدیر شبکه اجازه تطبیق پالیسی بالای کاربرهای شبکه را میدهد تا از طریق پراکسی (Proxy) دسترسی کامل به دیتا را داشته باشند.

انواع گروپ کاربر در دستگاه بلوکود:

- گروپ کاربر های محدود شده
- گروپ کاربرهای کنترول شده
- گروپ کاربرهای دسترسی کامل

کاربرهای جدید (User Account) که در شبکه وزارت امور داخله برای کارمندان ایجاد میگردد، ابتدا شامل گروپ محدود شده وبعدا به اساس درخواست وتایید اداره مربوطه نظر به ضروریات وظیفوی اجازه دسترسی به گروپ های دیگر را با طی مراحل نمودن اسناد قانونی حاصل مینماید.

مراحل باز شدن سایت های بلاک شده:

- کاربر باید درخواستی به مدیر مسئوول خویش به خاطر سایت های بلاک شده ارایه نماید.
- مدیر مسئوول باید درخواستی یورز را به ریاست عمومی مخابره و تکنالوژی معلوماتی راجع ساخته واحکام آن را اخذ نماید بعدا به بخش مدیریت ارتباطات استراتیژیک راجع گردد.
- بعد از احکام مدیر ارتباطات استراتیژیک و چک نمودن تیم تخنیکی در صورت عدم موانع امنیتی دسترسی به سایت های مذکور اجازه داده میشود.
- در صورت ختم قرارداد، اخراج وتقاعد کارمند یا نقض قوانین و پالیسی مخابره و تکنالوژی معلوماتی دسترسی کاربر به انترنت قطع و غیر فعال (Disable) میگردد.

- در صورت ختم قرارداد، اخراج وتقاعد کارمند یا نقض قوانین و پالیسی مخابره و تکنالوژی معلوماتی دسترسی کاربر به انترنت قطع و غیر فعال (Disable) میگردد.

به منظور مصؤن بودن شبکه وزارت امور داخله، گروپ کاربرهای دسترسی کامل (Full Access) بعد از 6 ماه بررسی گردد در صورت ضرورت مبرم بعد از ارایه پیشنهاد و تکمیل نمودن فورم دسترسی کامل (ضمیمه 3) از طرف اداره نیازمند برای 6 ماه دیگر تمدید میگردد.

مدیریت برنامه ها (Software Management)

به منظور افزایش استفاده بیشتر کارمندان وارایه خدمات حمایوی در عین زمان، تمامی کمپیوتر های وزارت امور داخله باید مجهز به برنامه های لازم باش. تا با استفاده از این برنامه کارمندان بتواند کارهای روزمره مربوط به وظیفه خویش را انجام دهند.

اجازه دادن کارمندان برای نصب نمودن برنامه ها در کمپیوترهایشان مشکلات زیادی را ببار خواهند آورد. نصب نمودن برنامه ها تو سط کارمندان در و سایل کمپیوتری مورد حمله گرفتن شبکه وزارت امور داخله تو سط افراد بیگانه به طور خوا سته یا نا خواسته قرار میگیرد. معرفی برنامه های مخرب از نصب و راه اندازی برنامه های آلوده شده، برنامه های بدون لایسنس (جواز) که میتوانند هنگام تفتیش کشف گردند وحتی پروگرام های که میتوانند برای هک کردن شبکه داخلی استفاده گردند مثال های از مشکلاتی میباشند که از طریق نصب برنامه ها توسط کارمندان به وجود میاید.

این طرزالعمل بالای تمامی کارمندان وزارت امور داخله و کمپیوتر های که از طریق اداره برایشان تهیه گردیده و به شبکه انترنت یا انترانت وزارت امور داخله دسترسی دارند تطبیق میگردد. همچنان این طرزالعمل شامل سرورها و دیگر وسایل کمپیوتری نیزمیگردد.

- کارمندان نباید هیچ نوع برنامه ها را در کمپیوترهای مربوط شبکه وزارت امور داخله نصب کنند.
- به صورت عموم، کارمندان حمایوی تکنالوژی معلوماتی برنامه های مجوز که در لیست تثبیت شده است روی هر کمپیوتر نصب نمایند بخاطریکه این برنامه های ضروری کارمندان را قادر به اجرا کارهای روزمره شان میسازند.
- هر برنامه ای که شامل لیست تثبیت شده نباشد تقاضای برنامه در قدم اول باید توسط اداره مربوطه و کارمند تکنالوژی معلوماتی تایید گردد وسپس به صورت کتبی به مدیریت شبکه یا تیم حمایوی تکنالوژی معلوماتی تحویل گردیده بعد از تثبیت تقاضا نصب برنامه اجرا گردد، تیم حمایوی تکنالوژی معلوماتی در قبال حمایه آن برنامه ها مسوولیت بعدی را نخواهد داشت.
- مدیریت شبکه تکنالوژی معلوماتی وظیفه بدست آوردن مجوزها (لیسانس) وپیگری آن، تست برنامه های جدید به خاطر جلوگیری از ناسازگاری وهماهنگی، واجرا نصب برنامه ها را به عهده دارد.
- اگر یک برنامه در داخل دومین (شبکه موجود) کار نمیکند پس کمپیوتر باید از دومین (شبکه موجود) خارج گردد وبه انترانت وزارت امور داخله دسترسی نداشته باشد.

لیست تصویب شده برنامه ها

- مایکروسافت ویندوز10 و 8
- مایکروسافت آفیس 2013 و 2016
- آنتی ویروس COMODO یا نوع دیگر تثبیت شده از طرف مدیریت ارتباطات استراتیژی
- برنامه Adobe Reader
- چاپگر و اسکنر
- دیکشنری دری و انگلیسی
- نت فریمورک 4.5

نرم افزار تائید نشده

هر برنامه دیگری که درلیست تصویب شده ذکر نگردیده است غیر قانونی است مگر اینکه توجیه مناسب به مدیریت شبکه تکنالوژی معلوماتی داده شود. علاوه براین مدیریت شبکه هیچ نوع پشتیبانی درقبال برنامه های تصویب ناشده را ندارد.

لایسنس (مجوز) برنامه ها

مدیریت کردن مجوزها مدیریت تکنالوژی معلوماتی را کمک میکند تا به طور کامل از اکثریت مجوزها استفاده صورت گیرد و سبب کاهش خریداری دوباره مجوز های برنامه در آینده گردد.

روشهای عمومی

کاربران مکلف اند تا از قوانین و پالیسی های تکنالوژی معلوماتی و مجوز برنامه ها پیروی کنند.

- در سیستم های تکنالوژی معلوماتی نباید هیچ نوع برنامه نصب یا استفاده گردد که متضاد با توافق نامه مجوز (license agreement) باشد.
- اسناد باید توسط کسانی که مسئوول مدیریت برنامه ها هستند نگهداری شود که مطمین شویم درهروقت اطلاعات مربوط مجوز در دسترس میباشد. همچنان یک کاپی اسناد دسترسی به معلومات، سایت ها ویا محدود ساختن اختیارات عموم وسایل شبکه به شمول تیلیفون های وایپ درنزد مدیریت سرورها وکاپی دیگر اسناد درمدیریت ارتباطات استراتیژیک حفاظت گردد.
- تمام پالیسی های که از طرف مدیریت ارتباطات استراتیژیک ترتیب گردیده باید به شکل گروپ پالیسی از طریق سرور برروی هر کاربرتطبیق گردد.

لیست برنامه های که باید نگهداری و به روز رسانی گردد.

- Microsoft Windows Server
- Microsoft Exchange Server
- Microsoft SharePoint
- AV & Application Whitelisting
- Backup system

مجوزهای که توسط بخش ICT مدیریت میگردد عبارتند از:

- تمام مجوز برنامه های که توسط مسولین شبکه یا بخش های دیگر استفاده میگردد باید خریداری ومدیریت گردد.
- لیست تمام مجوز برنامه باید ترتیب و به روز رسانی گردد و باید در دسترس مسولین شبکه و در شیرپوینت قرار گیرد.
- مسئوولین شبکه باید در مورد خریداری هرنوع برنامه مشوره و آگاهی دهند تا که از استفاده کامل و درست تمام مجوزهای در دست داشته اطمینان حاصل گردد.
- برنامه های که دارای مجوز نمی باشند باید عاجل تحت تطبیق (مجوز) قرار گرفته یا حذف گردد.

تطبیق مجوز برنامه ها

تیم حمایوی تکنالوژی معلوماتی مسئوول پالیسی نصب برنامه و تطبیق آن است. تحت هیچ نوع شرایطی تیم حمایوی تکنالوژی معلوماتی برنامه هایی را که در لیست تصویب شده ذگر نگردیده را نصب نخواهند کرد مگر اینکه توسط اداره پیشنهاد شده باشد و توسط مدیریت شبکه تائید گردیده باشد.

عدم تطبیق مجوز برنامه ها سبب موضوعات ذیل را خواهد داشت:

- مسئول تکنالوژی معلوماتی برنامه را از کمپیوتر کاربر حذف خواهد کرد.
- مسئوول تکنالوژی معلوماتی برای برنامه های که در لیست تصویب ذکر نگردیده است پشتیبانی نخواهد کرد.
- مسئوول تکنالوژی معلوماتی مسئوولیت هر نوع برنامه های تصویب ناشده را که در کمپیوتر کاربر باشد به عهده دارد.

تازه کردن (Update) مدیریت برنامه ها

مدیریت ارتباطات استراتیژیک ریاست عمومی مخابره و تکنالوژی معلوماتی حق اصلاح مدیریت برنامه ها را نظر به شرایط وتغییرات درمقطع زمانی را دارا میباشد. مدیریت شبکه تکنالوژی معلوماتی کوشش نهایی خویش را انجام دهند تا مطمین شوند که کاربران از تغییرات به وجود آمده با خبر شوند. در این حال باید جدید ترین نسخه مدیریت برنامه ها همیشه در دسترس و یا در شیرپاینت موجود باشد.

فصل سوم

مدیریت سیستم های معلوماتی(Information Management System)

دیتابیس و تنظیم خدمات الکترونیکی

مدیریت دیتابیس و تنظیم خدمات الکترونیکی با استقبال همه جانبه ازهمه دیتابیس های فعال مانند نیمز (NIMS) مربوط استخبارات، بایومتریک (Biometric) مربوط ریاست جنایی، کور آیمس (CoreIMS) مربوط ریاست لوژستیک، آپس (APPS) مربوط ریاست های عمومی مالی و بودجه و پیژنتون وآی دی کارت مربوط منابع بشری و سیستم های جدید که از طرف منابع مختلف مانند صندق وجهی پولیس (لتفا)، آسان خدمت و سیستیکا قرار داد و به وزارت امور داخله بمنظور تطبیق روند حکومت داری الکترونیکی وبه میان آوردن سهولت به شهروندان و کارمندان قوای پولیس ایجاد شده است، حمایت ونظارت می نماید.

مدیریت عمومی دیتابیس در راستای تحقق پلان های استراتیژیک وزارت امور داخله جهت بهبود روند کاری ادارات مربوط از دیتابیس های مذکور نظارت و ارزیابی می نمایید.

بمنظور تطبیق روند خدمات الکترونیکی و حمایه دیتابیس ها در سطح قطعات و جزوتام های وزارت امور داخله نکات آتی را ریاست های مربوطه، تمویل کننده ها وقرار داد کننده گان در نظر داشته باشند.

بخش اول

پالیسی امنیتی دیتابیس و سیستم ها

امنیت سیستم به معنی حفاظت از دیتا(معلومات) در مقابل افراد واشخاص غیرمسئوول است. بخاطر اطمینان ادارات ذیربط مطابق اصل شفافیت وحسابدهی مراجع اجرا کننده برنامه وحفظ اسرار ادارات وقطعات وجز تام های وزارت امور داخله با در نظرداشت قوانین نافذه، لوایح و تعلیم نامه ها صورت گیرد تا باشد سیستم های ایجاد شده و در حالت ساخت وساز به مشکلات و حملات سایبری مواجه نگردند. در سیستم های دیتابیس محدودیت هایی وضع گردد از آمدن تغییرات ناخواسته توسط افراد جلوگیری بعمل آید.

مفاهیم اصلی امنیت معلومات

امنیت دیتا(معلومات) به چهار بخش کلی در نظر گرفته شود:

- محرمیت (Confidentiality): یعنی حفاظت از معلومات درمقابل دسترسی واستفاده افراد غیر مسئوول.
- درست بودن (Integrity): به این معناست که دیتا نباید توسط افراد غیرمسئوول ایجاد، تغییر ویا حذف گردند.
- دقت (Authenticity and Validity): دلالت برموثق بودن معلومات (دیتاها) ونیز اصل بودن آنها دارد، به طریقی که اطمینان حاصل شود که معلومات کاپی یا جعلی نیستند.
- دسترسی (Availability): به این معنی که معلومات دیتابیس و سیستم ها در زمان نیاز در دسترس باشند.

بنابراین موارد فوق الذکر امنیت معلومات ودیتابیس را جداً مراعات نمایند.

مطابق پلان های وزارت امور داخله وقوانین نافذه کشور نگهداری اسرار بخش سکتور امنیتی ومعلوماتی توسط ادارات ذیربط جدا مراعات گردیده ودرخصوص حفظ معلومات دیتابیس ها با بخش قرارداد کننده و هیئت تخنیکی شان در حضورداشت مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره تفهیم ومتعهد گردیده تا اسرار حفظ گردد در غیر آنصورت مطابق قانون مسئوول میباشند.

امنیت کلی سیستم در مراحل دیزاین، برنامه نویسی، پیاده سازی و حفظ و مراقبت آن توسط ترتیب کننده و توسعه دهنده سیستم ها (شرکت ترتیب کننده وادرات ذیربط وزارت امور داخله) به صورت جدی در نظر گرفته شود.

همه کارمندان مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی مکلف به اجرای وظایف محوله مطابق به لایحه وظایف شان میباشند.

بخش دوم

ظرفیت سازی مدیریت ها و کارمندان سیستم های دیتابیس

برنامه آموزشی وظرفیت سازی یک امر ضروری ومهم برای کارمندان هراداره میباشد که مطابق قانون، ظرفیت سازی در شروع وجریان اجراات کاری قرار ذیل در نظر گرفته شود:

- در صورتیکه تغییرات در سیستم عامل یا (سیستم عامل) کمپیوترهای مورد استفاده اداره مربوطه صورت میگیرد.

- مطابق بازار کار، سیستم عامل های جدید با کارآیی بهترو امنیت بیشتر از طرف شرکت های مربوطه تکنالوژی در بازارعرضه میگردد. بنا هرگاه سیستم عامل مطابق نیازمندیهای اداره خریداری ودر کمپیوترهای مربوطه نصب میگردد، برای کاربرد بهتر و مناسب سیستم عامل ها برنامه های آموزشی برای کارمندان اداره در نظر گرفته شود.
- در صورتیکه دیتابیس جدیدی برای اداره ایجاد و یا توسعه میابد.
- در صورتیکه تغییرات در قسمتهای مختلف سیستم دیتابیس موجود اداره بوجود بیاید.

در هردو مورد فوق الذکر برنامه های آموزشی و ظرفیت سازی برای کارمندان طوری صورت گیرد که:

- آموزش های تخنیکی دیتابیس ترتیب شده به پرسونل تخنیکی مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی با تفاهم مدیریت مربوطه در نظر گرفته شده تا روند بهتر تطبیق گردد.
- آموزش سیستم جدید برای کارمندان(End User)با تفاهم مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی ترتیب و ارائه گردد.

بخش سوم

ترتیب وایجاد سیستم دیتابیس

عقد قرارداد های پروژه ایجاد دیتابیس و سیستم مورد استفاده

- درحین عقد قرارداد دیتابیس ها ویا خدمات الکترونیکی باید نماینده ریاست عمومی مخابره و تکنالوژی معلوماتی حضور فعال داشته باشد تا درهنگام انتقال مسئوولیت هابه وزارت امور داخله دچار مشکلات تخنیکی نگرد در غیر آن مسئولیت های بعدی آن متوجه مرجع قرارداد کننده میباشد.
- حین عقد قراردادهای خدمات الکترونیکی (دیتابیس ها) یک کمیته تخنیکی مشترک از ادارات ذیربط توظیف گردد.
- پلان منظم از سروی الی روند واگذاری دیتابیس ها با تفاهم وهماهنگی مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی قبل ازقبل ترتیب گردد تا در قسمت حمایت بعدی اجراات صورت گیرد.
- کلیه مالیات و منابع پولی قرارداد بخش دیتابیس ها بدوش شرکت قرارداد کننده میباشد.
- هیچ یک از پرداخت خسارات ناشی از، از بین رفتن و یا مفقود شدن منابع مادی ومعنوی بصورت عمدی، سهوی یا بی پروایی بالای قیمت ایجاد وتوسعه پروِژه دیتابیس تاثیرات ندارند وبدوش قرارداد کننده میباشد.
- توافق روی تسلیم دهی Source Code(منبع کود) دیتابیس ها و پروگرام ها فی مابین قرارداد کننده و وزارت امور داخله صورت گیرد.
- مرجع پرداخت وجوه مالی خرید License(جواز) تکنالوژی های مورد نیاز درحین عقد قرارداد مشخص گردد.
- توافق روی حفظ ومراقبت و ضمانت (Warranty) کارکرد سیستم مطابق به نیازمندی های ادارات ذیربط صورت گیرد.

تحلیل و دیزاین دیتابیس

مشخصات سخت افزاری سیستم دیتابیس نظر به کارایی باید مطابق استانداردهای روز در نظر گرفته شود.

دیزاین دیتابیس باید به مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی ازطرف ترتیب کننده دیتابیس شریک شود، و توسط کمیته تخنیکی ریاست عمومی مخابره و تکنالوژی معلوماتی تائید شود.

برنامه نویسی و توسعه سیستم

ارزیابی پروگرام های توسعه یافته بمنظور اطمینان از تطبیق استانداردها ومعیارهای برنامه نویسی در وزارت امور داخله می باشد. اسناد تخنیکی دیتابیس و برنامه ها باید به مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی ازطرف ترتیب کننده دیتابیس شریک گردیده ومورد تایید کمیته تخنیکی ریاست عمومی مخابره و تکنالوژی معلوماتی قرار گیرد.

اصول، قوانین و استندردهای برنامه نویسی بمنظور کار کرد و عملکرد بهتر سیستم در نظر گرفته شود.

تطبیق و بهره برداری سیستم

در روند تطبیق خدمات الکترونیکی و دیتابیس های قطعات و جزوتامهای وزارت امور داخله نماینده مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی حضور فعال داشته باشد که درآینده بعد از واگذاری سیستم به مشکلات و چالش ها مواجه نگردد.

یو ای تی User Acceptance Test (UAT) وسایر تست های مورد نیاز باید با تفاهم مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی برگذار گردد.

تمام Database Demo ها باید با تفاهم مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی ارائه گردد.

اسناد ذیل باید از طرف ترتیب کننده دیتابیس به مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی تسلیم داده شوند:

- Source Code Technical Documents.
- Source Code Review Documents.
- Administrative Documents.
- Business Flow Documents.
- Data Dictionaries.
- Data Flow Diagrams.
- Entity Relational Diagrams.
- Use Case Diagram.
- Sequence Diagram.

سورس کود Source Code از طرف ترتیب کننده دیتابیس به مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی تسلیم داده شود.

سورس کود Source Code پیش از تسلیم دادن باید تست شود.

درصورت توافق، جواز (License) تمام تکنالوژی ها به مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی تسلیم داده شود.

مراقبت سیستم وفراهم نمودن خدمات بعد از تطبیق

عقد قرارداد های حفظ و مراقبت سیستم ها باید تحت کنترول و نظارت مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی صورت گیرد.

مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی بحیث مرجع مسئوول بعد از دریافت پیشنهاد ادارات ذیربط بخاطر ایجاد تغییر مطابق نیاز درسیستم ها (دیتابیس واپلیکیشن) مربوطه شان، موضوع را بررسی نموده واجرااات می نماید.

بخش چهارم

مسؤلیت های بخشهای مربوطه مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی

برای فعال نگهداشتن ادارات که با سیستم های کمپیوتری(دیتابیس وآپلیکشن) تجهیز گردیده اند بخش های مربوطه مدیریت عمومی دیتابیس و تنظیم خدمات الکترونیکی، ریاست عمومی مخابره و تکنالوژی معلوماتی قرارذیل فعالیت مینمایند:

- مدیریت، توسعه و تنظیم پروسه ثبت معلومات اداری در سیستم های مربوطه.
- تأمین ارتباط وهمآهنگی موثر با ادارات ذیربط در مورد مشکلات و توسعه دیتابیس و شریک ساختن هر نوع مشکلات و تغییرات تخنیکی سیستم ها با مراجع ذیصلاح برای بهبود اجرااات سیستم ها.
- اشتراک در جلسات تخنیکی با ادارات مربوطه و مشاورین سیستیکا برای کارایی بهتر وبیشتر سیستم های مربوطه.
- توسعه سیستم مطابق نیازمندی ادارات مربوطه به منظور بهبود سیستم های ارتباطی و تکنالوژی معلوماتی و ایجاد سهولت های کاری در عرصه های مختلف.
- نظارت و ارزیابی معلومات وارد شده در دیتابیس ها.
- کنترول، تجزیه و تحلیل مشکلات تخنیکی سیستم ها.
- مدیریت وکنترول کاربران خدمات سیستم ها.
- مدیریت و کنترول Back up یا تهیه کاپی معلومات دیتابیس و سیستم های معلوماتی.
- مدیریت امنیت و محافظت سیستم های معلوماتی و معلومات ذخیره شده در سیستم ها.
- ارائه گذارش از دست آوردها به صورت هفته وار، ماهوار و ربع وار به مدیریت عمومی دیتابیس وتنظیم خدمات الکترونیکی.
- اجرای وظایف مطابق لایحه وظایف که از طرف اداره مربوطه سپرده میشود.
- تنظیم نمودن طرزالعملهای مناسب به منظور کارایی، توسعه سرعت و تغییرپذیری سیستم های دیتابیس و اپلکیشن در سطح وزارت امور داخله.
- توسعه بخش پالیسی دسترسی و مدیریت دیتابیس های ترتیب شده درسطح قطعات و جزوتام های وزارت امور داخله.

فصل چهارم

ارتباطات تاکتیکی

مسؤولیت های مدیریت عمومی مخابره ارتباطات تاکتیکی

تأمین ارتباطات مخابروی قطعات و جزوتام های قوای پولیس ملی افغان با در نظر دا شت سل سله مراتب صورت می گیرد. تمام ارتباطات از مرکز واحد اداره گردیده و گزارش اجراات ســـاعت وار، روزانه، هفته وار تابع قید زمان ومکان معیین می باشد.

- آمریت مخابره سـوق واداره صـرف مسـئوولیت ارتباطات مخابروی مراکزهماهنگی (OCCP، OCCDو OCCR) (مرکز هماهنگی ولسوالی، مرکزهماهنگی ولایت، مرکزهماهنگی ساحوي) وهمچنان مسئوولین قطارهای اکمالاتی و حالات خاص را بدوش دارد.
- شبکه های مخابروي طور ربع وار کود گذاري میگردد. در صورت نیاز در ماه یکبار تغییر داده میشود. کود شبکه (اسم کود واحد: اسم پارولا 0060) به حروف و عدد ترتیب میشود.
- به منظورجلوگیري از مداخله و پخش پرازیت در ارتباطات مخابروي دوربرد (HF) پروسه ثبت و پروگرام نمودن فریکانس در د ستگاه های مخابروي مذکور صرف از سل سله مدیریت فریکونسی و مایکرویو و در هماهنگی مدیریت عمومی مراکز مخابره مجازبوده هیچ اداره و جزوتام حق تغییرات خود سرانه را در زمینه ندارد.
- درصورت تقاضا مبنی برپروگرام نمودن دستگاه (HF) حسب ضرورت قطعات شامل کود شبکه مخابره مرکز و ولایات شده بعد از طی مراحل قانونی ثبت فریکونسی میگردد.
- ریاست ها و اپارات مرکزي که شامل کود شبکه نیستند حق ثبت وپروگرام دستگاه های مخابره های UHF (واکی تاکی)خود را در رپیترهای اپارات مرکزي ندارند.
- هیچ اداره بدون ارتباط وظیفوي و یا موافقه قوماندانی امنیه کابل و حوزه های امنیتی مربوط به آن حق ثبت و پروگرام فریکونسی حوزات امنیتی وقوماندانی امنیه کابل را در مخابره های واکی تاکی (UHF) ندارد.
- کنترول رادیویی عبارت از استعمال واستفاده دقیق و تثبیت شده قواعد مکالمات بی سیم ازطرف موظفین مربوط میباشد که به موثریت آن توجه جدي مبذول گردد.
- د سپلین رادیویی عبارت ازمراعات دقیق مقررات ا ستفاده ازد ستگاه مخابره بی سیم، جلوگیری از مکالمات متن باز و سایر تخلفات دسپیلین رادیویی که کشف مکالمات رادیویی را برای دشمن آسان ومساعد ساخته و تأمین ارتباط اطمینان بخش را در میدان محاربه بین قطعات وجزوتام ها م شکل ساخته، میبا شد. این ا صل یکی از وظایف مهم وا سا سی من سوبین مخابره بوده آن را جداً مراعات نمایند.
- تمام منسـوبین پولیس ملی که از وسـایل مخابروي اسـتفاده مینمایند حق ندارند به سـایر شـبکه ها بدون مجوز قانونی مداخله نمایند.

پروسه استندرد عملیات

بخاطر ایجاد بهبود و تداوم بهتر پروسه عملیاتی، مشق و تمرین مخابروي مطمئین و دوامدار نکات آتی بالترتیب در نظر گرفته شود:

- تمام سیستم های مخابروي قطعات وجزوتام ها از نگاه چینل، تیپ مود، فریکانس، قدرت، با هم مطابقت داشته باشد.
- تمام دستگاه های مخابروي، ساحه مخابره مشترك داشته باشند.
- تمام لینهای (کیبل های) ارتباط از نقطه نظر دیدگاه انجنیري تحکیم و به صورت دقیق وصل گردیده باشد.
- سیستم مخابروي باید موثریت عالی داشته و به صورت دوامدار فعالیت کرده بتواند همیشه فعال باشد.
- سیستم مخابروي فوق العاده ستر اخفاء گردد واز کشف رادیویی دشمن محفوظ باشد.

توسعه و تطبیق پروتوکول های مشترك سیستم مخابروی

سیستم مخابره پولیس ملی

مطابق پروتوکول و طرزالعمل مشترك بین ارگانهای امنیتی تأمین ارتباط بصورت منظم از محل قومانده با قرارگاه ها و جزوتام های مربوط صورت گیرد. این نوع تأمین ارتباط در یک زمان دقیق به اساس استعجـالیت وظیفوي ازطرف ارگانهای مربوط تشریک مساعی (هماهنگی) گردیده وبه وسیله دستگاه های (U.H.F-VH-HF) تأمین ارتباط میگردد.

ساختار سوق واداره

غرض سوق و اداره بهتر قوت ها و تأمین ارتباطات مخابروي تدابیر ذیل اتخاذ گردد:

- نگهداری روحیه پرسونل و احضارات محاربوی دوامدار قطعات و جزوتام های مخابره در اثنا تأمین ارتباط مخابره.
- ترتیب پلان ارتباط مخابره در اثنا محاربه.
- تعیین وظایف برای قطعات وجزوتامهای مخابره در وقت و زمان آن.
- تأمین ارتباطات دوامدار و بدون سکتگی قواي پولیس.
- اجرای مانوربا قوا و وسایل مخابره واکمال کردن احتیاجات احتیاطی مصرف شده مخابره در وقت و زمان آن.
- کنترول دوامدار ارتباط مخابره وتأمین فعالیت دوامدارآن با سایردستگاههای مخابره.
- تنظیم امورتعلیم و تربیه پرسونل قطعات و جزوتام های مخابره با در نظرداشت وسایل پیشرفته و تکنالوژی جدید که به دسترس قرار میگیرد.
- اکمال تخنیکی جزوتامهای مخابره.
- حفظ و مراقبت حالت تخنیکی و سایل مخابروي در هنگام وظیفه بدوش نوکریوالان موظف بوده و کنترول بررسی از حالت تخنیکی وسایل متذکره در مرکز بدوش آمرین مراکز و مدیر عمومی مراکز مخابره میباشد.
- حفظ و مراقبت حالت تخنیکی وسایل مخابروي در هنگام وظیفه در ولایات بدوش مدیر ومعاون مخابره قوماندانی های امنیه ولایات میباشد.

محرم سازی ارتباطات شفر

مدیریت محرم سازی ارتباطات درچوکات ریاست عمومی مخابره و تکنالوژی معلوماتی باطرح وتطبیق پالیسی ها، پروسیجرهاوپلانها با درنظرداشت نیازمندیهای محرمیت ارتباطات، وظیفه طبقه بندي اسرار، اسناد، معلومات، محرمیت سایرمنابع معلوماتی و جلوگیري ازافشأ اسرارنظامی رابه عهده دارد.

این بسیار مهم است که شعبات محرم سازي ارتباطات در مرکز و محلات یک محیط کاملا مصئون مناسب ومحفوظ باشند و از ورود اشخاص غیرمسئوول به داخل شعبات جداً ممانعت شود و تمام اسناد محرم درسیف ها و آلماریهای فلزي محکم ومطمین جابجا و مهر ولاك گردد.

غرض حفظ مصئونیت اسناد محرم تدابیر مشخص اتخاذ و پیگیري شود تا از بحران ها، تهدیدات و واقعات ناگوار به سیستم های ارتباطی و معلوماتی جلوگیري شود.

در سراسر جهان استفاده از وسایل تکنالوژی معلوماتی سهولت های زیاد را در ساحات امنیتی و خدماتی بوجود آورده است. بمنظور استفاده موثراز وسایل مذکور وجلوگیري از رسیدن آسیب ها به آن، ایجاب می نماید تا تدابیر لازم درین زمینه اتخاذ گردد.

عوامل ذیل بخشی از عواملی است که باعث رسیدن آسیب ها به سیستم ارتباطی و معلوماتی شفري میگردد:

- عدم طبقه بندي اسناد وعدم رعایت درجه محرمیت.
- عدم مشخص ساختن مسوولیت ها در زمینه عدم اخذ تضمینات افراد ومنسوبین که به اسناد ومعلومات دسترسی دارند و یا استخدام میشوند.
- محافظه و تنظیم نادرست اسناد و معلومات.
- عدم تطبیق پالیسی های محرم سازي.
- استفاده ازفلش ها(چیپ ها) وعدم بلاك کردن پورت یوایس بی.
- صلاحیت اشتراك در گروپها و سایت های غیرمجاز کاربر های شامل تشکیل شفر.
- استفاده از رمزهای عبوری ساده بصورت دوامدار.
- استفاده از حساب کاربر یک منسوب توسط شخص دیگر.
- عدم ممانعت از ورود اشخاص غیرمسئوول به دفاتر اسناد محرم.
- اعطاي صلاحیت دسترسی به منابع بدون تعقیب و نظارت.
- نداشتن مسئوولین مشخص بمنظور اداره و تنظیم منابـع و اسرار اشد محرم به سطح ادارات و جزوتامها.

پروسه های محرم سازي

هرنوع سند و یا مکتوب، جداول و غیره اسناد محرم که ترتیب میشود صرف به تعداد کاپی که ضرور است تهیه شده و به اشخاص مشخص مسئوول تسلیم یا ایمیل گردد. کاپی که اضافه باشد ازبین برده شده و یا محفوظ شود. برای از بین بردن کاپی اضافی و یا خاکه در دفاتر که به اسناد اشد محرم سروکار دارد، باید تریشر(خوردکننده کاغذ) موجود باشد تا اوراق را از بین ببرد، ترتیب کننده اسناد فوق در قسمت بالائی آن درجه محرمیت را به شکل ذیل تعیین می نماید:

- درجه محرمیت (اشد محرم).
- درجه محرمیت (محرم غرض استفاده رسمی).

این اسناد چه ازطریق ایمیل بشکل الکترونیکی باشد یا غیرالکترونیکی، شخص گیرنده مطابق درجه محرمیت درحصه محافظه واجرااات آن مسئوول خواهد بود.

محرم سازي سیستم های ارتباطی

ارتباطات ستراتیژیک که متشکل از سیستم اوت لوك (ایمیل ها)، تیلفونهای محرم (وایپ) ویدیو کنفرانسها است از طریق نصب سافت ویرهای معتبر محرم سازي مانند (جی.پی.جی) ویا بهتر و پیشرفته از آن استفاده شده تا معلومات که به دسترس شخص غیرمسئوول قرار میگیرد قابل استفاده نبوده و به شکل کود نشان داده میشود، صرف مسئوولین که دسترسی شان مجاز باشد از سیستم مذکور استفاده کرده میتوانند.

- رمز عبوری یا رمز استفاده از کمپیوترها محرم نگهداشته شود ودارای ترکیب مغلق باشد تا امکان دسترسی شخص دیگر به آن محدود گردد.
- سی دي روم کمپیوترها بمنظور داخل ساختن و کاپی کردن برنامه ها و معلـــــومات بصورت غیر مجاز، بلاك میباشـد.
- اسنـاد صلاحیت های دسترسی به سیستم ها و منابع بشکل مسئوولانه ترتیب و مطابق به وظایف تطبیق و رعایت گردند.
- محدودیت های تیلیفون های آی پی محرم وایپ طوري باشد که تأمین ارتباط بین منسوبین وزارت امورداخله به وسایل مشابه یعنی از تیلیفون وایپ به وایپ صورت گیرد.
- شفافیت ومحافظه (IP) پروتوکول های توزیع شده شبکه برای بخش شفر ها محرم نگهداشته شود.
- اسناد معلوماتی بشمول رهنماي تیلیفونها و ایمیل آدرس ها صرف بمنظوراجراي امور رسمی درداخل وزارت امورداخله استفاده شود.
- هر کاربر یا ارسال کننده و اخذ کننده ایمیل ها امضا الکترونیکی مشخص داشته باشد تا احساس مسئوولیت پذیري بلند برده شده و پروسه تثبیت افراد تقویت و ساده گردد.

سیستم اداره منابع ارتباطی ومعلوماتی اشد محرم

این منابع شامل اسناد، ریکاردها، دفاتر، دیتا(معلومات بشکل الکترونیکی) و سایر معلومات مهم و ضروري میباشد که بشکل ذیل باید تنظیم و اداره گردد:

- هرجزوتام (اداره) باید یک نفر را بحیث مسئوول و یک نفر را بحیث معاون تنظیم، حفظ و اداره معلومات اشد محرم برعلاوه ازوظایف اصلی شان تعیین و توظیف نماید.
- مسئوولین تنظیم و اداره معلومات محرم، به منظورفراگیري وحاصل کردن رهنمودهای محرم سازي به مدیریت عمومی شفر معرفی میگردند تا رهنمائی های لازم در رابطه به سیستم محرم سازي و کودهای مشخص برای شان صورت گیرد.
- مسئوولین مذکور تضمین معلومات اسناد مشخص را برای واگذار ساختن مسئوولیت ها برای اشخاص که با اسناد و معلومات در اداره مربوطه شان دسترسی دارند ترتیب و برایشان با در نظرداشت مسئوولیت وظیفوي تفویض صلاحیت صورت میگیرد.
- مسئوولین مذکور شیوه های معین و مشخص را برای ایجاد یا اخذ منابع معلومات واسناد، نشر، ارسال، شریک ساختن، تازه کردن (آپدیت)، ذخیره کردن، تعیین دوره حیات، فهرست الی از بین بردن یا محوکردن معلوماتی اشد محرم را بدوش دارند.

مدیریت محرم سازی ارتباطات مکلف است تا پلان های مشخص را برای بازدید از ارگانهای شفري ولایات تحت اثر آن ها بخاطر جلوگیري از چالش ها در مقابل کار پرسونل ولایات کشور وجلوگیري از نفوذ شبکه های جاسوسی کشور های خارجی و دشمنان داخلی داشته باشد.

ریاست عمومی مخابره و تکنالوژی معلوماتی مکلف است، تا پلان های مشخص وعملی را به منظوراعزام هیات های موظف که غرض بازدید و بررسی شعبات شفري قوماندانی های امنیه ولایت وسایرقطعات وجزوتام های پولیس ملی به خاطرجلوگیري از ایجاد مشکلات درراستاي کاري پرسونل شعبات مذکور، مقابله با نفوذ شبکه های جاسوسی کشورهای خارجی ودشمنان داخلی اعزام میگردند،اتخاذ نمایند.

ایمیل های که در سطح شبکه وزارت امور داخله تبادله میگردد باید توسط نرم افزار خاص یا سرتیفیکت (Certificate Authority) رمزگزاری (Encrypt) گردد. برای رمزگزاری کردن ایمیل ها از نرم افزار PGP یا GPG استفاده کرد.

نرم افزار(Software) رمزگزاری بدون تایید و ارزیابی مدیریت ارتباطات استراتیژیک (NOC) و کارشناسان مدیریت مربوط صورت گرفته نمیتواند.

فصل پنجم

حمایوی

پروگرام های تعلیمات مسلکی

واضح و هویدا است که ترتیب وتطبیق پلان های همه جانبه ودقیق باعث موفقیت قطعات وجزوتام ها در وظایف محوله شان میگردد. وازجانب دیگر تربیه کادرهای تخصصی با معیارهای ملی وبین المللی دررشته های تکنالوژی معلوماتی ومخابراتی یک امر ضروري بوده رشد و توسعه استعداد های فکري و مهارتهای مسلکی مشخص با کادرها رکن اساسی و ادامه حیات مسلکی را تشکیل میدهد. بر وفق هدایات، اوامر واولویت های کاري مقام وزرات اموراخله، پلانها وپالیسی های پولیس ملی پیرامون اخذ تدابیر و ترتیب پلانهای کاري درازمدت و کوتاه مدت در رابطه به پیشبرد دروس وآموزش پروگرام های مختلف ابتدایی و پیشرفته (Basic & Advanced) مخابره و تکنالوژی معلوماتی برای تمام پرسونل شامل تشکیل مخابره و تکنالوژی معلوماتی وافراد پولیس که از وسایل مخابروي و کمپیوتري وسایر وسایل الکترونیکی درجزوتام های مرکز وولایات مربوط پولیس ملی وزارت اموراخله استفاده مینمایند. مدیریت عمومی پروگرام های تعلیمی ریاست عمومی مخابره و تکنالوژی معلوماتی (ICT) به منظور اجراي خدمات مسلکی مخابره و تکنالوژی معلوماتی، استفاده موثر دوامدار ولاینقطع ارتباطات مخابروي و الکترونیکی، دایرکتیف ها، اوامر ودساتیر وزارت امور داخله اهداف مشخص را دنبال می نماید. این طرزالعمل بمنظور ارتقاي سطح دانش مسلکی، قابلیت ها، توسعه ظرفیتها وفعالیت های مسلکی (مخابره و تکنالوژی معلوماتی) درامور اجراي وظایف امنیتی و خدماتی و زارت امور داخله درهرنوع شرایط برای شناختن مسئولیت های اساسی، ایجاد پروسیجر ها وپالیسی های مشخص برای بخش های مختلف، آموزش و تعلیمات مسلکی جهت بدست آوردن مقاصد ودیدگاه های استراتیژیک ذیل طرح گردیده است.

- سراسري ساختن آموزش تعلیمات مسلکی مخابره و تکنالوژی معلوماتی برای تمام قواي پولیس.
- سرعت عمل درامور پیشبرد آموزش و تعلیمات مسلکی.
- فسخ قرارداد های شرکت های آموزشی بیرونی جهت جلوگیري ازمصارف زیاد درتوسعه وظرفیت سازي نیروي پولیس ملی (استادان) درصورت توسعه تشکیل بخش ساحوي.
- توسعه وتوسعه فعالیت های تعلیمات مسلکی وایجاد محلات تدریسی جدید.
- ارتقای ظرفیتها، قابلیتها ومهارتهای مسلکی قواي پولیس غرض استفاده درست و بموقع از وسایل مخابروي کمپیوتري وسایر وسایل الکترونیکی مربوط به تکنالوژی معلوماتی معاصر.
- انتخاب وگزینش پرسونل مسلکی مورد ضرورت از فارغان کورسهای متذکره در ادارات مربوط.
- تقویت رهبري وتنظیم اموروایجاد اداره سالم فاقد فساد اداري.
- سازماندهی، توسعه وتقویت فعالیت پرسونل درخصوص نظم و دسپلین، رعایت واحترام به مسلک نظامی، مسئوولیت پذیري با شایستگی وجلب اعتماد مردم بالای قواي پولیس ملی.

ریاست عمومی مخابره و تکنالوژی معلوماتی وزارت امور داخله برعلاوه از اجراي وظایف تأمین امنیت مردم وظیفه ارائه خدمات درعرصه استفاده ازوسایل مخابروي و تکنالوژی معلوماتی را نیز به عهده داشته که بخاطر اجراي بهتر وبه موقع امورمتذکره فعالیت های ذیل را انجام میدهد:

- آموزش تعلیمات مسلکی وارائه خدمات سیستم های ارتباطی قواي پولیس به منظور طرز استفاده درست و بموقع از وسایل الکترونیکی ومخابروي تکنالوژی معلوماتی.
- آموزش پروگرامهای ابتدایی وپیشرفته وسایل تأمین ارتباطات مخابروي و تکنالوژی معلوماتی وسایر وسایل الکترونیکی برای تمام منسوبین قواي پولیس وکارمندان درسطوح مختلف وزارت امور داخله که با وسایل تکنالوژی معلوماتی وارتباطی دسترسی کامل داشته باشند.
- آموزش تعلیمات مسلکی مطابق مسلک بطور جداگانه، ارائه خدمات جهت آموختن روش های محرم سازي وشفر، شبکه ناك (انترنیت، نتورکینگ)، فکس، کیبلنگ و دیتابیس ها.
- آموزش وتدریس تعلیمات مسلکی، طرز حفظ ومراقبت و نگهداشت تمام وسایل ارتباطی والکترونیکی تکنالوژی معلوماتی.
- آموزش تعلیمات مسلکی کمره های امنیتی وکنترولی، اسکنرها (تلاشی بدنی)، قراول ها، غرض کنترول وتعقیب ترافیک جاده های اطراف قطعات وجزوتامهای وزارت امور داخله، مرزهای کشور و افراد(پرسونل ومراجعین).
- آموزش تعلیمات مسلکی جهت ارائه خدمات سیستم منابع بشری (دیتابیس ایرمز).
- آموزش وتدریس لسان انگلیسی بمنظور ارتقا دانش، استفاده درست از وسایل الکترونیکی و تکنالوژی معلوماتی و رفع ضرورتها ومشکلات لسانی.
- بمنظور توسعه فعالیت ها، ارتقا ظرفیت وتوسعه استفاده از تکنالوژی معلوماتی ایجاد مراکز آموزشی درمحلات ومناطق که ضرورت محسوس میگردد.

شرایط فعال سازي مراکز آموزشی و آمادگی استادان

بمنظور ایجاد صنوف تدریسی مطالب ذیل در نظرگرفته شود:

- معرفی آموزگاران بخش های ارتباطات رادیویی مخابروي، الکترونیکی، محرم سازي درکورسهای ارتقا ظرفیت مسلکی بمنظور خود کفایی.
- ایجاد مراکز آموزشی درقرارگاه ریاست عمومی مخابره و تکنالوژی معلوماتی قرارگاه های قطعات و جزوتامهای بزرگ و مستقل مرکزي و محلات پولیس ملی افغانستان.
- افزایش و توسعه مراکز آموزشی سیستم های وسایل ارتباطات مخابروي، الکترونیکی و محرم به کتگوری های مختلف مسلکی در قطعات و جزوتامهای قواي پولیس.
- صنف درسی حد اقل گنجایش تعداد (20) نفر را داشته باشد.
- صنف درسی مجهز با میز، چوکی وسیستم انرژي برق باشد.
- صنف درسی داراي پورتهای انترنیتی بوده و با نتورك وصل باشد.
- صنف درسی با مواد درسی (کمپیوترهای مکمل الاسباب، انواع مخابره ها وسایر وسایل الکترونیکی) مجهز باشد.
- دروس هر دوره مدت دوازده هفته را احتوا میکند.
- در ختم دوره برای هرمداوم فارغ شده تصدیق نامه توزیع میگردد.

اکمالات:

هیچ یکی از عینیات (اجناس) مخابروي عامه قابل فروش، تحفه دهی، قرضه دهی، مبادله ویا مورد استفاده شخصی نمیباشد جزاینکه قانون اجازه آنراداده باشد. درصورت مفقودي، خساره و یا تخریب عینیات و اجناس مخابروي جبران خساره آن طبق طرزالعمل جداگانه سنجش و به حساب دولت انتقال میشود. هر منسوب نظامی که از عینیات (جنس) مخابروي، دولتی استفاده مینماید، مسئوول مراقبت، نگهداري و محافظت آن میباشد پرسونل جمع دهی (معتمدین) نباید به وظایف دیگري طور خدمتی توظیف گردند تا از ایجاد سکتگی در وظایف محوله شان جلوگیري بعمل آمده باشد.

توزیع کریدت کارت به اساس ضرورت و انجام وظایف غرض تأمین ارتباطات تیلیفونی منسوبین قواي پولیس ملی صورت گیرد. توزیع وسایل مصرفی از قبیل (کریدت کارت ها، تونرباب وغیره)از دیپو برویت فورم (10)صورت میگیرد.

پروسه های اکمالاتی:

- دفترداري.
- استرداد وسایل.
- تثبیت احتیاج.
- تسلیمی اجناس دفترداري.

دفترمحاسبوي خوب ومنظم اساس موفقیت یک اداره یا جزوتام راتشکیل می دهد. مسئوولین ازطریق مراجعه به دفاتر، اسناد، معلومات وارقام مورد نیاز را بصورت عاجل بدست آورده پلانها وتصامیم عملیات ها را طرح ریزي مینمایند. دفترداري نامنظم وعدم مسئوولیت پذیری، بازپرس ومجازات را درقبال دارد.

برای تنظیم اموردفترداري شرایط ذیل بایدمراعات گردد:

- تمام اسناد فورمه جات وکتاب های املاك طبق تعلیمات نامه عینیات امور لوژستیکی عیار وتنظیم گردد.
- تمام اوراق، کتب، املاك و دفاتر مربوطه مهر، ثبت، شماره گذاري شده و داراي پوش محفوظ و مناسب باشد.
- دفاتر و فورم های مربوطه باید بشکل درست محافظه شود تا از تخریب، دستکاري، سرقت و حریق محفوظ باشند.
- فورم های اکمال، توزیع واسترداد بدون تاخیر در جریان سه روز در دفاتر معامله گردد.
- هرنوع عینیات لوژستیکی که از هر مرجع اکمال و یا به دسترس اداره بخش های ارتباطی قرار میگیرد در دفاتر مربوطه معامله جمع و قید شود.
- اجناس و وسایل مورد ضرورت قطعات و جزوتامهای قواي پولیس بدون اسناد اصولی از دیپو داخل و خارج شده نمیتواند.
- دفاتر به اساس مکتوب رسمی بعداز دوره تسلیمی به محاسبین تسلیم داده شود، منسوبین که بحیث محاسب و معتمد تعیین میگردند توانایی فکري و استعداد شان ارزیابی و در نظرگرفته شود. درقبال دفاتر املاك و اسناد محاسبوي، آمرین کنترول اوپراتیفی نموده تا محاسبات را بشکل احسن و شفاف آن صورت گیرد.

استرداد وسایل

درشرایط ذیل استرداد وسایل به شکل انفرادي صورت میگیرد:

درصورت تبدیلی، ترك وظیفه، تقاعد وتحصیلات درازمدت و درخواست منسوبین وسایل بعد از نظر هئیت و تنزیل کتگوري عملیه استرداد وسایل و جمعدهی به معتمد صورت میگیرد وبه اساس فورمهای درخواست طبق کتگوري به منسوبین دوباره توزیع میشود.

وسایل که بعد از نظر هئیت تخنیکی (ورکشاپ) وآمر اعطا برویت فورم (63) قابل ترمیم نبوده و یا مصارف ترمیم از 50% تجاوز میکند بعد از تخلیه اسرار و فارمت کردن به اساس فورم (71) درکتگوري 4، 5 استرداد میشود.

طرز تخلیه دیپوها یا گدام ها و دفاتر از وسایل استرداد شده غیرقابل استفاده کتگوري 4،5

وسایل که به اساس نظریه تخنیکی مندرج فورم (63) داخل دیپو گردیده باید مطابق طرزالعمل از سیستم محاسبه و دیپو خارج و به اساس پیشنهاد مدیریت اکمال ریاست عمومی مخابره و تکنالوژی معلوماتی وحکم مقامات وزار ت امورداخله و توظیف هئیت لیلام، حریق و دفن گردند.

وسایل حافظه دار(هاردسک) و یا ثبت فریکانس نظامی در صورت امکان فارمت و یا کشیده شوند تا استفاده از آن غیر ممکن گردد.

تثبیت احتیاج

تثبیت احتیاج یک عنصر عمده برای رفع نیازمندي قطعات و ادارات دولتی بوده و باید طبق سنجش درست و استوار به اسناد ومعلومات مستند صورت گیرد.

درآغاز ربع (3) سال مالی درخواست تثبیت احتیاج از طریق مرجع مربوطه کتباً به جزوتامها و ادارات طبق تشکیل منظور شده ارایه شود وجداول تثبیت احتیاج جزوتام ها با درنظرداشت معیاد معینه به مدیریت عمومی اکمال ریاست عمومی مخابره و تکنالوژی معلوماتی ارسال گردد.

نحوه تثبیت احتیاج

- مطابق تشکیل وضرورت قطعات.
- تثبیت تعداد وسایل که عارضه دار گردیده و ترمیم شان امکان نداشته باشد.
- تثبیت تعداد وسایل که در جریان محاربه و حملات دشمن تخریب یا تلف شده باشد.
- در نظر گرفتن فیصدي مشخص وسایل احتیاطی به منظور حمایه عملیاتها و وظایف فوق العاده.
- تعداد وسایل که دوره حیات (لایف سایکل) شان تکمیل گردیده و یا سال آینده تکمیل میگردد.
- پرزه جات و ادوات فالتو شامل بطري ها، چارجرها و غیره به منظور حفظ و مراقبت.
- اجناس مصرفی از قبیل کارتریجها، تونرباب، درم ها، بالتی و غیره نظر به مصارف سالهای گذشته و با درنظرداشت وسایل جدید.
- موجودي وسایل جدید یا استرداد شده که قابلیت استفاده را دارا میباشد از تثبیت احتیاج تفریق گردد.

شیوه توحید نیازمندیها ازطرف مدیریت عمومی اکمالات به شکلی صورت میگیرد که جداول نیازمندیها درمقایسه با تشکیل موجود، سطح اکمال، تشکیل جدید، راپورهای وسایل عارضه دار استرداد شده، وسایل تلف شده، مصارفات سالهای گذشته وبا درنظرگرفتن فیصدي وسایل ریزرف به منظورحمایه عملیات ها و وظایف فوق العاده طوراحتیاطی بعد ازمعلومات اجناس موجود در دیپوهای جزوتام های مربوطه و مشخصات که برای اجناس ارایه شده ارزیابی شده ووسایل که بعد ازمحاسبه تطابق به شرایط فوق و مشخصات درج شده تثبیت میشوند درتوحید عـمومی بحیث تثبیت احتیاج ریاست عمومی مخابره و تکنالوژی معلوماتی تثبیت میگردد.

دوره حیات (Life Cycle)

وسایل وتجهیزات مخابروي وکمپیوتري درقدم اول مربوط به طرز استفاده پرسونل مربوطه بوده که درحفظ ومراقبت ان سعی وکوشش به خرچ دهند در صورت سهل انگاري، عدم استفاده مسلکی، مفقود شدن جنس، عدم موجودیت دیپوهای االستندرد ومسلکی، عدم نگهداشت ومحافظت اجناس دردیپوها مسئوولین تحت باز پرس قانونی قرار میگیرند ومدیریت ورکشاپ مرکزي درهماهنگی با ورکشاپ های محلی وولایتی سیمینار های میتودیک حفظ ومراقبت را دایر وپرسونل را اگاه نماید و نیز با در نظر داشت کتگوري وسایل (معیادي و مصرفی) ذیلاً اقدام صورت گیرد.

وسایل و تجهیزات معیادی

الف - وسایل و تجهیزات معیادی و استفاده مؤثر

وسایط ووسایل، تجهیزات معیادي، وسایل مخابروي نصب سیستم های مختلف ارتباطی و تکنالوژی معلوماتی، سرورها وسایر وسایل پرارزش به اساس پیشهناد بخش اکمالاتی هرسه سال یک بارازطرف هیئت تخنیکی ومتخصص معاینه وسروي گردد از صحت بودن جنس اطمینان حاصل و در صورت بروز خطرات ومشکلات به ترمیم وتعویض پرزه جات الی تعویض مکمل جنس متذکره درمطابقت با تعلیمات نامه عینیات لوژستیکی اقدام نمایند.

ب - وسایل و تجهیزات معیادی تاریخ تولید جنس الی تاریخ انقضأ جنس

ازینکه تمام پرزه جات، آلات، وسایل وتجهیزات کمپیوتري ومخابروي از طرف شرکت تولید کننده االستندرد و معیادي میباشد و دوره حیات آن از تاریخ تولید محاسبه میگردد نه ازتاریخ استفاده، بناً در وقت تسلیمی اجناس قرارداد شده وداخل نمودن آن به دیپو تحت نظر هیئت مشترك مشاهده صورت گیرد تا از تاریخ تولید آن بیشتر از 6 ماه سپري نشده باشد.

ج - وسایل و تجهیزات معیادی سروي سالانه گروپ تخنیکی ومتخصص

در این حالت بطور سالانه در جنب هیئت تثبیت احتیاج اجناس نظر به پیشنهاد بخش اکمالاتی یک گروپ هیئت تخنیکی ومتخصص تعیین و توظیف گردند تا از صورت استفاده یا عدم استفاده وسایل وتجهیزات که شامل بخش الف و ب نبوده سروي و نظریات موثر خویش را مطابق مواد (17 الی 174) تعلیمات نامه عینیات لوژستیکی ابراز نماید تا برویت آن در تعویض وسایل وتجهیزات اقدام صورت گیرد.

اجناس و وسایل مصرفی

مسئوول اکمال بخش مرکزي مکلفیت دارد در مورد ختم دوره حیات وسایل و اجناس کمپیوتري و مخابروي تحت نظر هیئت مسلکی و تخنیکی هر دوبخش مطابق تعلیمات نامه عینیات لوژستیکی طرزالعمل مشخص برای هرنوع جنس ترتیب و مورد اجراً قرار دهند.

دوره حیات وسایل وتجهیزات این بخش با در نظر داشت تاریخ تولید وانقضا تحت نظر وملاحظه هیئت تخنیکی سنجش صورت گیرد ودرتعویض وتبدیل نمودن آن مطابق تعلیمات نامه عینیات لوژستیکی و تخنیکی و (تعیین معیاد) اقدام صورت میگیرد.

بودجه و قرارداد ها

برنامه های موثر وهدفمند درتقویت، اکمال وتجهیز نیروهای پولیس ملی از نظر ارتباطات موثر الکترونیکی، ارتباطات محرم مخابروي وتوسعه شبکه نقش محوري واساسی را ایفا میکند. پالیسی مذکور درروشنایی قانون مالیات برعایدات، قانون تدارکات وطرزالعمل تدارکات عامه تدوین گردد.

مدیریت بودجه وقرار داد ها جهت بهبود روند کاري ومصرف موثربودجه منظورشده، پالیسی مالی و تدارکاتی خویش را بادرنظرداشت مطالب ذیل ترتیب می نماید:

- ترتیب پلان تدارکاتی سالانه به اساس نیازمندي (تثبیت احتیاج) جزوتامها درهماهنگی با جزوتام مربوطه ومدیریت اکمالات.
- اولویت بندي پروژه ها وقرارداد ها به اساس اهمیت و ارجحیت آنها.
- ترتیب وتنظیم اسناد قرارداد مطابق شرطنامه های مشرح به مشوره مستقیم بخش سفارش دهنده غرض شفافیت ومسئوولیت پذیري شرکت قرارداد کننده.
- پلان مصارفاتی (مالی) طبق برنامه های پلان تدارکاتی آماده گردد..
- پرداخت جداول زمان بندي شده به اساس پلان مالی.
- نظارت دوامدار از وضعیت قرارداد ها وپروژه های این ریاست با در نظرداشت راپور کیفیت شعبه مربوطه از اجرا وعدم اجرای مواد قرارداد جهت تنظیم وزمان بندي بموقع مطابق شرطنامه صورت می گیرد.
- حصول اطمینان ازمطابقت قرارداد ها طبق پلان تدارکاتی وتادیات طبق پلان مالی انجام می پذیرد.
- هماهنگی با ریاست عمومی تدارکات (خریداري) و ریاست عمومی مالی وبودجه.
- اجراي حواله جات طبق پلان مالی(پرداخت تادیات وقرارداد های که خارج از پلان تدارکاتی باشد) اهمیت وارجحیت آن توسط متخصصین اموربررسی گردیده در صورتیکه از اهمیت خاص برخوردار نباشد، ازاجراي آن صرف نظر بعمل می آید.
- تنظیم بودجه وارسال تخصیصات به ولایات و مراجع ذیربط دیگر به اساس اولویت ونیاز در اغاز سال مالی بعد از منظوري بودجه صورت می گیرد.

بخش کادري مخابره و تکنالوژی معلوماتی

مدیریت پیژند درچوکات ریاست عمومی مخابره و تکنالوژی معلوماتی مسوولیت ها ونظارتهای تشکیلاتی و تعییناتی افراد را برای بخشها وسیستم های ارتباطی و تکنالوژی معلوماتی بدوش داشته که ازطریق طرح پالیسی ها، پروسیجرها وپلانهای توسعهی زمینه انتخاب وعزل ونصب افرادواجد شرایط را میسرمیسازد.

- ابرازموافقه مبنی برتقرر افراد واجد شرایط مطابق مسلک ازطریق بورد مشورتی ریاست عمومی مخابره و تکنالوژی معلوماتی بعد از ارزیابی اسناد تحصیلی واخذ امتحان صورت میگیرد.
- ریاست عمومی مخابره و تکنالوژی معلوماتی با در نظرداشت رشد وتوسعه تکنالوژی زمینه جذب و استخدام افراد واجد شرایط را آماده و بعد ازپروسه شناسایی درمورد استخدام شان ازسلسله ریاست پیژنتون اقدام می نماید.
- به منظور ایجاد قابلیت ها، بالا بردن ظرفیت ها، حفظ محرمیت درامور محوله وصرفه جویی در بودجه افراد مسلکی تربیه وجاگزین افراد موقتی قراردادي میگردند تا محرمیت شناسایی افراد مناسب که ازعهده انجام وظایف تأمین ارتباطات حفظ ومراقبت, ترمیمات، اداره سیستم ها واستفاده ازوسایل تکنالوژی معلوماتی به شکل موثر آن بدرآمده بتواند، حفظ گردیده باشد.
- معرفی منسوبین واجد شرایط به مراکز آموزشی و مسلکی.
- ارایه پیشنهادات مبنی بر توسعه تشکیل بخش ارتباطات و تکنالوژی معلوماتی با درنظرداشت پلان توسعهی.
- مرورتشکیلات موجود وارزیابی هربست از طریق بورد مشورتی.
- ترتیب وتنظیم لایحه وظایف مشخص به هربخش وارایه دلایل برای تغییرات با در نظرداشت خصوصیات وظیفوي هر بست.
- ارزیابی پرسونل بخش های ارتباطی و تکنالوژی معلوماتی طور شش ماهه وسالانه.
- استخدام وجذب افراد متخصص شامل انجنیري تکنالوژی معلوماتی، انجنیران ورکشاپ و استادان مسلکی از موسسات تحصیلات عالی خصوصی ودولتی درهماهنگی با ریاست عمومی پیژنتون، ریاست منابع بشری ودرصورت ضرورت تعدیل رتبه ازرتبه ملکی به رتبه نظامی با رعایت ماده (86) قانون امور ذاتی افسران، بریدملان وساتنمنان صورت میگیرد.
- بخاطر جلوگیري از نفوذ دشمن درخصوص عزل و نصب کدر های مخابره و تکنالوژی با استفاده از شیوه های (فورم های تضمین خط، وشناخت با استفاده از راه بلد ها، نقاط نیرنگی منازل، سوابق کاري و جرمی) درهماهنگی با ارگان های کشفی و استخباراتی اجراات صورت گیرد.
- کمپیوترایز نمودن اسناد ذاتی افسران، ساتنمنان، سربازان، مامورین ملکی واجیران در دیتابیس ایرمز و آپس (AHRIMS & APPS) درهماهنگی با ریاست عمومی پیژنتون با در نظر داشت محرمیت اسناد بطور دوامدار پیگري میگردد.
- درج وثبت شهرت مکمل افراد شرکت های قراردادي، ترتیب استعلام های دخولی وخروجی به قرارگاه مربوط، ترتیب فورم های ضمانت افراد بمنظور جلوگیري از نفوذ دشمن.

در بخش سوق و اداره سیمدار

- مدیریت سوق و اداره سیمدار ارتباطات تیلیفون های دیجیتل (سیمدار و بی سیم) را درسطح مرکز و ولایات، قطعات وجزوتامهای قواي پولیس ملی تأمین مینماید وتوسعه آن الی سطح ولایات درنظر میباشد.
- فعال نگهداشتن ورفع عوارض عاجل ودوامدار، تیلیفون های دیجیتل توسط پرسونل و نوکریوالان 24 ساعته صورت می گیرد.

- طی مراحل اصولی اسناد نمرات عارضه دار غرض فعال نمودن و ترمیم آن.
- توزیع نمرات جدید دیجیتل بعد ازطی مراحل اصولی اسناد صورت میگیرد.
- ازتیلیفون های دیجیتل دست داشته در امور رسمی استفاده صورت گیرد.
- در جریان یک ماه مصرف اضافه از(6000) افغانی یک شماره تیلیفون دیجیتل قابل مجرایی نبوده البته با در نظر داشت استعجالیت وظیفوي در سه کتگوري (2000-4000-6000)تنظیم گردد.
- با در نظر داشت استعجالیت و حجم وظایف اوپراتیفی، نوکریوالی های اوپراتیفی ومراکز مخابره مرکز و ولایات شامل محدودیت مصرف نورم نمیباشد.
- قبل از کندن کاري جوار تعمیرات قطعات و جزوتامهای قواي پولیس با ریاست عمومی مخابره و تکنالوژی معلوماتی و مدیریت های مخابره قطعات وجزوتامهای قواي پولیس تفاهم وهماهنگی صورت گیرد.
- تعمیرات که جدیداً اعمار میگردد سیستم لین دوانی وجین بکس تیلیفون ها مانند لین دوانی سیستم برق در نظر گرفته شود وشامل نقشه ساختمان وتعمیر گردد.
- ترتیب، تنظیم واصلاحات درچاپ رهنماي نمرات تیلیفون ها وآدرس های الکترونیکی منسوبین قواي پولیس سال دومرتبه صورت گیرد، در صورت تغییر وتبدیل مسولین شامل رهنما از طریق آدرس الکترونیکی اخبار گردد.
- رهنماي تیلیفون که طرف استفاده منسوبین قواي پولیس قرار دارد در حفظ محرمیت آن توجه جدي صورت گیرد.
- با بدسترس قرار گرفتن سیم کارت های (MOI) قطعات وجزوتامهای وزارت امور داخله غرض جلوگیري ازمصارف گزاف از آن استفاده اعظمی نمایند.

وظایف و مکلفیت های بخش کمره های امنیتی

اجراات سالم وکنترول دایمی از ساحات تحت مسئولیت، کشف و دریافت متخلفین، جلوگیري ازبروز واقعات و ریکارد نمودن رویداد ها بمنظور تحکیم حاکمیت دولتی و امنیت ساحه تحت مسئوولیت.

سروي، نصب، عیار سازي ونصبیشن کمره های امنیتی مطابق طرزالعمل در قطعات و جزوتامهای مرکزي ومربوط قواي پولیس با تفاهم مسئوولین مربوطه جهت تثبیت محل و بمنظور کنترول ساحات تحت مسولیت بخاطر جلوگیري از واقعات وتثبیت اشخاص مشکوك.

ثبت و ریکارد رویداد ها

- فعال نگهداشتن دوامدار سیستم کمره های امنیتی بر حسب ضرورت.
- مراقبت از سیستم اخذ اطلاعات ذخیره شده.
- ذخیره نمودن وکاپی گرفتن (بک آپ) واقعات و رویداد ها توسط شخص مسئوول.
- حفظ ومراقبت، ارزیابی ونظارت دوامدار از سیستم کیبل های تمدید یافته، کمره ها، ادپترها، ال سی دي و اسکرین ها توسط موظفین ومسئوولین ساحه.
- توظیف پرسونل مسلکی امریت مخابره و تکنالوژی قطعه مربوطه و نوکریوال موظف بطور 24 ساعته غرض نظارت ومراقبت کمره های امنیتی در ساحه تحت مسئوولیت.
- موظفین که به سیستم دسترسی دارند در خصوص محرمیت رمز عبوری ها، حفظ و نگهداشت معلومات (دیتا) ثبت شده، قبل از فارمت شدن معلومات مکلفیت دارند.

- در صورت وقوع کدام حادثه به اشخاص غیرمسئوول اجازه دست زدن به سیستم حافظه داده نشود.
- مسئوول کمره های امنیتی در صورت خاموش شدن کمره ها، ساعت قطع ریکارد را الی دوباره فعال شدن ریکارد رسماً به کتاب نوکریوالی درج وعلت ان را نیز ذکر نماید.
- مسئوول کمره های امنیتی درمحضر هیئت سه نفري تعیین شده و امر مشخص قوماندان (امر بک آپ) گرفته میتواند.
- در صورت بروز عوارض تخنیکی در سیستم از دست زدن اشخاص غیر مسئول و غیر فنی جلوگیري. وسایل مورد ضرورت کمره های امنیتی قطعات درج فورم (14) شده وبعد از طی مراحل قانونی آن در جمع معتمد مدیریت مخابره قطعه توزیع و بعد از نصب، اسناد مصارفاتی ان طبق تعلیماتنامه به مرجع مربوطه ان ارایه وهمچنان توزیع، اکمال و جمع و قید وسایل و تجهیزات کمره های امنیتی از قبیل دستگاه دي وي آر، ال سی دي، اسکرین، یو پی اس، کیبورد، ریموت، به شکل معیادي و وسایل و تجهیزات از قبیل کیبل برق، کیبل تصویر، کلپ، دبل و پیچ جین بکس، رابرتیپ وغیره بطور مصرفی بعد از نصب و نصبیشن جمع وقید دفتر ومعامله گردد.

بخش ارتباطات استراتیژیک شبکه جزوتام ها

تحت رهنمود مستقیم مدیریت مخابره و تکنالوژی معلوماتی، پالیسی وپروسیجرهای طرح شده ازطرف مسوولین بخش شبکه و تکنالوژی معلوماتی که درضمیمه (5) تذکر یافته طرح گردیده باشد مسوولیت ها ونظارتهای ذیل را بدوش دارد:

- تأمین ارتباطات دوامدار وراپورگیري از ادارات مربوطه و راپوردهنده به شبکه مرکزي ریاست عمومی مخابره و تکنالوژی معلوماتی ازطریق سیستم (اوتلوك) شبکه اخذ وارسال ایمیل ها، ویدیوکنفرانسها، تیلیفونهای وایپ واستفاده سایت شیرپواینت بدون محدودیت تشکیلاتی زون و یاخارج از زون شبکوي.
- نظارت وهمکاري با مدیربخش مربوطه درزمینه توسعه قابلیت هایپرسونل، آموزش ها دربخش شبکه و تکنالوژی معلوماتی به سطح جزوتام مربوطه.
- نظارت وتطبیق پالیسی های که بمنظورحفاظت شبکه از انواع آسیب ها و تهدیدها طرح گردیده است.
- کنترول و اتخاذ تدابیر موثر امنیتی بمنظورحمایه سایر وسایل شبکه بشمول سرورها.
- جلوگیري ازسواستفاده وخدمات که بمنظوراستفاده قانونی ورسمی فراهم گردیده است.
- تنظیم امورمربوط به کارمندان (انجینران) آي تی در وظایف روزمره واستفاده ازتجارب شان.
- کنترول و نظارت ازنحوه پیشبرد پروگرامهای آموزشی تکنالوژی معلوماتی وشبکه به سطح جزوتام.
- ذخیره، مراقبت واداره منابع معلوماتی به سطح ادارات وجزوتامهای مربوطه در ساحه.

انتخاب افراد برای پیشبرد وظایف ارتباطات

تحت رهنمود مستقیم مدیریت مخابره و تکنالوژی معلوماتی وپالیسی وپروسیجرهای طرح شده ازطرف مسئولین مدیریت پیژند که درضمیمه (6) تذکریافته مسئوولیت ها و نظارتهای ذیل رابدوش دارد:

- درانتخاب افراد برای بست های بخشهای ارتباطات سپري نمودن پروسه که شامل اعلان، جمع آوري اسناد مانند تحصیلات مسلکی، تجارب کاري و ارزیابی باشد.
- پالیسی مکافات ومجازات تعقیب شود یعنی پرسونل که ازخود در اجراي وظایف ابتکار وشایستگی نشان میدهند به امتیازات تشویقی پیشنهاد وپرسونل که دراجراي وظایف غفلت وسهـــل انگاري نموده باشد مطابق قانون ومقرارت مجازات میگردند.

صلاحیت های نظارتی و واگذاری مسئوولیت ها

تمام مسئوولین به منظورحصول اهداف اساسی غرض تأمین وحمایه بهترمکلف به مسئوولیت پذیري ونظارت ازبخش های مربوطه شان طبق جدول ضمیمه (5) قرار ذیل میباشند:

1- صلاحیت نظارتی ومسئولیت های ریاست عمومی مخابره و تکنالوژی معلوماتی ومعاون آن

ریاست عمومی مخابره و تکنالوژی معلوماتی ومعاون آن وظایف شانرا با در نظرداشت لایحه وظایف، دیدگاه ها واهداف ستراتیژیک وزارت امورداخله طبق هدایات وپلانهای مرتبه معینیت ارشد امور امنیتی ومقامات وزارت امورداخله تنظیم نموده رهبري وزارت امورداخله رامطمئن میسازندکه وضیعت سیستم ارتباطات وتسهیلات (منابع) آن به موثرترین ومناسب ترین وجه محافظت، تنظیم واداره میگردد.

در رأستاي تحقق مدرنیزه سازي، تجهیز و ارتقأ ظرفیت های فنی ومسلکی بشکل علمی وتدریجی به مقامات وزارت امورداخله مشوره وزمینه سازي مینمایند.

بحیث رهبران و اداره کننده گان عموم بخشهای ارتباطات وزارت امورداخله ایفاي وظیفه مینمایند.

سایر بخش ها و مدیریت های مربوطه را متوجه به رعایت وعملی کردن پالیسی ها، پروسیجرها و پلانها نموده و رهنمایی های لازم مینمایند.

ازطریق اعزام وتوظیف ساختن هئیت ها به منظور موجودي ها، طرزاستفاده های معقول وارزیابی های فنی ومسلکی طبق پلان مرتبه ازتمام سطوح ارتباطات وقدمه ها نظارت مینمایند.

گزارشهای کاری سایر بخشهای ارتباطات را مطابق لایحه وظایف، طبق پلان مطالبه و ارزیابی می نماید.

پالیسی سطح مکافات ومجازات پرسونل را درتمام بخشهای ارتباطات نظارت نموده زمینه ارتقاي ظرفیت ها، رتب وسایر امتیازات مسئوولین را فراهم میکنند ودرصورت ارتکاب تخطی ها، غفلت وضعف، تصامیم مقتضی را اتخاذ مینمایند. بحیث آمرین اعطا بخش های ارتباطات تمام پروسه ها و اجراات روزمره راکنترول، مرور ومنظور مینمایند.

2- صلاحیت های نظارتی ومسئولیت های مدیریت اداره تنظیم وفریکونسی

اداره وتنظیم فریکونسی، جلوگیري از مداخلات، استفاده غیر قانونی از آن، حفظ ونگهداشت واستفاده سالم از تمام فریکونسی های توزیع شده را به عهده دارد.

- بدون درخواست و توزیع فریکونسی از طریق مدیریت عمومی تنظیم و اداره فریکونسی هیچ یک از پرسونل پولیس ملی افغانستان نمیتواند فریکونسی را دردستگاه های خود تغییر وثبت نماید.
- بدون رنج (دایره) فریکونسی پولیس و درصورت ضرورت ازمشترك ملکی ونظامی، از دیگر رنج ها استفاده کـــرده نمیتوانند.
- کاربر وسایل مخابروي مطابق پالیسی فریکونسی هذا بدون هدایت ودعوت به سایـــــر فریکونسیها داخل شده نمیتواند.
- هیچ یک از پرسونل تنظیم واداره فریکونسی حق دادن فریکونسی را به هیچ یک از ارگانهای دولتی، غیردولتی، اشخاص وشرکت های خصوصی ندارد.

- منسوبین پولیس ملی که از وسایل مخابروي استفاده مینمایند حفظ ومحرمیت را درنظر گرفته از افشا فریکونسی پولیس ملی جداً اجتناب ورزند.
- بدون سلسله مدیریت تنظیم و اداره فریکونسی هیچ یک از پرسونل پولیس ملی حق انتقال، تغییر و تبدیل و نصب ریپیتر(Repeater) جدید را ندارند.
- هیچ یک از پرسونل حق تغییر فریکونسی ریپیتر ها وسایر وسایل مخابروي را ندارند.
- مسئوول ارتباط در زمان پرواز طیاره الی نشست به هیچ صورت حق دور شدن از دستگاه و خارج شدن از شبـــکه را ندارد.
- پروگرام نمودن فریکونسی و وسایل مخابروي UHF VHF HF صرف از طریق مسئوولین مدیریت عمومی فریکونسی صورت گرفته میتواند.
- بمنظور حفظ محرمیت فریکونسی قواي پولیس منبعد قراردادي ها وسایر ادارات موسسات داخلی وخارجی که وسایل مخابروي را مطابق قرارداد و یا کمک بدسترس قواي پولیس قرار میدهند، حق ثبت و پروگرام نمودن دستگاه های مذکور را ندارند.

سیمکارت تیلیفون های مبایل، که طرف استفاده منسوبین دولتی وغیر دولتی قرار دارند باید ثبت و راجستر گردند و راجستر کننده در قبال آن مسئوولیت دارد تا ازسیمکارت مشخص اش شخص دیگر استفاده ننماید در صورت مفقودي بطور عاجل به مرجع مربوطه اطلاع دهد تاصلاحیت تماس سیمکارت متذکره قطع شده و در صورت نیاز مثنی آن گرفته شود.

3- صلاحیت های نظارتی ومسئولیت های بخش شبکه و تکنالوژی

- مسئوولین شبکه و تکنالوژی معلوماتی تحت رهبري مستقیم ریاست عمومی مخابره و تکنالوژی قدمه های معینیت ارشد امور امنیتی ومقامات وزارت امورداخله تمام وظایف تأمین ارتباطات استراتیژیک ومرکز اصلی عملیات یا دوماین(شبکه) اصلی و تکنالوژی معلوماتی را به عهده دارد.
- طرح وتطبیق پالیسی ها، پروگرامها، توسعه شبکه، اداره منابع معلوماتی وحفاظت شبکه ازخطرات و آسیب ها را به سطح وزارت امورداخله پیگیري مینمایند.
- مسئوول، مراقبت وکنترول استفاده معقول و رسمی از وسایل تکنالوژی و شبکه به سطح وزارت امورداخله بوده جلو استفاده های سو وغیرقانونی رامیگیرند. سو استفاده ازاملاك دولتی (استفاده شخصی، غیرقانونی به نفع سازمانها، تجارت وغیره) شمرده میشود.

4- صلاحیت های نظارتی ومسئولیت های مدیریت عمومی اکمالات

مسئوولین مدیریت عمومی اکمالات تحت رهبري مستقیم ریاست مخابره و تکنالوژی معلوماتی و قدمه های معینیت ارشد امور امنیتی و مقامات وزارت امورداخله بوده وظایف اکمال و توزیع وسایل مخابروي و تکنالوژی معلوماتی سیستم نظارتی و محاسبوي رابه سطح مرکز وتشکیلات ساحوي از طریق طرح پالیسی ها، پروسیجرها درمطابقت باقوانین وتعلیماتنامه های عینیات لوژستیکی بدوش دارند.

تمام وسایل مخابروي، شبکه، تکنالوژی معلوماتی و سیستم های ارتباطی صرف از یک مرجع اکمال و توزیع میشود درصورتیکه وسایل ازکدام طریق دیگراکمال شود درآنصورت مشکلات در سیستم حفظ و مراقبت پرزه جات، سازگاري با سیستم های شبکه،آموزش ها وسیستم مخابروي ایجاد خواهد شد.

5- صلاحیت نظارتی محاسبوی وجوابدهی بخش اکمال وتوزیع وسایل مخابروی، شبکه وتکنالوجی معلوماتی

تحت رهنمود مستقیم مدیریت مخابره و تکنالوژی معلوماتی با درنظرداشت قوانین نافذه کشور وپالیسی وپروسیجرهای طرح شده ازطرف مسئولین مدیریت عمومی اکمالات که درضمیمه (6) تذکر یافته طرح گردیده باشد مسئوولیت هاونظارتهای ذیل رابدوش دارد:

- اکمال وتوزیع وسایل معیادي، مصرفی وپرزه جات مورد ضرورت بخشهای ارتباطات طبق نیازمندي.
- ایجادسیستم منظم وشفاف حسابدهی.
- جلوگیري ازحیف ومیل وسایل ارتباطی.
- تثبیت احتیاج وسایل.
- استرداد وسایل.

6- صلاحیت نظارتی ومسئولیت های مدیریت مخابره و تکنالوژی معلوماتی ق، ا، ولایات وجزوتام ها

- سوق، اداره ورهبري عموم پرسونل بخشهای مربوط ارتباطات به سطح جزوتام اعم از پرسونل رسمی ویا قراردي.
- تطبیق مجموع پالیسی ها، پروسیجرها و پلانهای که ازطرف مسوولین مندرج ضمایم(5) و(6) طرح گردیده باشد.
- فراهم سازي تسهیلات برای حمایه سیستم ارتباطات ادارات وجزوتامهای وابسته به تشکیلات وزارت امورداخله بدون درنظرداشت تشکیلات قدمه، جزوتام و یا خارج ازآن.
- تثبیت احتیاج وسایل وپرزه جات مربوط بخش ارتباطات دراربع (سوم) برای سال بعدي در هماهنگی با مدیریت اکمالات ریاست عمومی مخابره و تکنالوژی معلوماتی.
- پیشنهاد بودجه (تخصیص) برای بخش های ارتباطات درهماهنگی با مدیریت بودجه و قرار داد های ریاست عمومی مخابره و تکنالوژی معلوماتی.
- تأمین ومروج سازي ارتباطات استراتیژیک بین ادارات وجزوتامهای مربوطه و قرارگاه وزارت امورداخله با استفاده ازشبکه ساحوي سیستم اوت لوك اخذ، ارسال، اداره وذخیره ایمیل های مربوط به وظایف رسمی وعملیات ها.
- رهبري سیستم تنظیم واداره منابع معلوماتی طبق رهنمود پالیسی مشخص منابع معلوماتی به سطح ادارات وجزوتامهای مربوطه.
- نظارت ازتطبیق پروگرامهای آموزشی عموم پرسونل و توسعه پروگرامهای تخصصی برای پرسونل بخشهای ارتباطات.
- اطمینان ومتیقن ساختن رهبري ریاست عمومی مخابره و تکنالوژی معلوماتی درنهایت مقامات وزارت امورداخله ازاینکه تأمین وحمایه سیستم ارتباطات و وسایل مربوطه درتمام قدمه های تحت اثر به موثرترین و بهترین وجه محافظه ومورد استفاده قراردارند.
- انتخاب افراد شایسته ومناسب برای تعیینات در بخش ارتباطات.

7- صلاحیت های نظارتی ومسئولیت های مسئوولین حفظ ومراقبت ورکشاپ

مدیریت ورکشاپ در چوکات ریاست عمومی مخابره و تکنالوژی معلوماتی مسئوولیت حفظ، مراقبت، ترمیم وطرزانتقال معقول از وسایل مخابروي، شبکه و تکنالوژی معلوماتی، شیوه های موثر را از طریق ایجاد و تنظیم ورکشاپ های مرکزي وساحوي طبق اهداف استراتیژیک و پلانهای منظور شده مقام وزارت امور داخله به عهده دارد. حفظ ومراقبت (ترمیم) فعالیت وسایل رابیشتر ساخته دراجراي وظایف روزمره سهولت ها را ایجاد مینماید. به منظور تبدیلی پرزه جات وسایل عارضه دار که قابل ترمیم نمیباشد تثبیت احتیاج ذیلاً صورت گیرد:

به اساس تعداد و انواع توزیعات جدید که از طریق مدیریت عمومی اکمالات صورت میگیرد باید پرزه جات که از نگاه تخنیکی وفنی داراي اسیب پذیري درجات (1، 2، 3) هستند تعداد شان نظر به درجه اسیب پذیري ضم جدول تثبیت احتیاج گردد.

نظر به ترمیمات وسایل که از قبل به دسترس جزوتامها قرار داده شده است مطابق اسناد تبدیلی پرزه جات وترمیم میزان شش ماهه ویک ساله را مرور وجمع بندي کرده نیازمندي برای سال آینده تثبیت میگردد.

تمام پرزه جات موجود در دیپوي ورکشاپ مرکزي وساحوي موجودي شده طبق راپورکه کدام نوع پرزه جات چه تعداد در کدام ورکشاپ موجود است نظر به موجودیت نیازمندي پلان تثبیت احتیاج مشخص میگردد.

بعد از ملاحظه ومقایسه جداول مرتبه تمام ورکشـــاپ های مرکزي وساحوي تثبیت احتیاج فوق، با در نظرداشت حقایق و شواهدی که از راپور ها گرفته شده نتایج نهایی بعد از ارزیابی از طریق هیئت تخنیکی به مدیریت بودجه و قرارداد ها ارسال میگردد.

ترمیمات یا برطرف ساختن عوارض و مشکلات در وسایل مخابروي و تکنالوژی ایجاب اقدامات فوري و عاجل را مینماید که بایددرکمترین فرصت ونزدیکترین محل به طریقه ذیل صورت گیرد:

درصورت مشکلات ویا انقطاع درفعالیت وسایل مخابروي و کمپیوتري نزد کاربر که ازمحل ورکشاپ دورباشد ازطریق تماس به تیلیفونهای محلات حمایتی(Help desk) مشکل را انتقال دهد تا ازطریق مراجع حمایتی رهنمائی لازم تیلیفونی برایشان صورت گیرد.

وسایل مخابروي و کمپیوتري ازطریق خودشخص، اشخاص غیرفنی یاغیرمسئوول درورکشاپهای شخصی باز و بسته و ترمیم نشوند.

وسایل مخابروي و کمپیوتري که نیازبه ترمیم دارند درابتدا ازطرف مسئوولین مربوطه ارزیابی میشودکه آیا به اثرکدام عوامل عارضه دارگردیده اند طورمثال:

- حملات تخریبی دشمن.
- حادثات ترافیکی وآفات طبیعی.
- درجریان استفاده وفعالیت زیاد بشکل تدریجی.
- غفلت، استفاده ناسالم ویا طورعمدي ازطرف کاربر یا مسئوول.

بعدازتثبیت عوامل فوق با اتخاذ تدابیر واجرااات لازمه درصورتیکه ترمیم درورکشاپ بخش مخابره و تکنالوژی لازم باشدفورم (63) ترمیم وسایل ترتیب شده ازطرف شعبه عایده به ملاحظه شدآمرین اعطا مربوطه شان بعد از ثبت به بخش ورکشاپ ارسال شود.

بخش ورکشاپ های ساحوي و مرکزي درابتدا اطمینان حاصل نمایدکه وسیله واقعاًمربوط به عینیات دولتی (وزارت امورداخله) بوده، بعداً آنراتثبیت عوارض نموده وبه هئیت تخنیکی که به اساس هدایت رسمی آمرین ویا قوماندانان مربوطه طور(ربعوار)توظیف می گردند با توضیح مطالب ذیل راجع و محول می سازد.

وسایل عارضه دار توسط سه نفرهیئت تخنیکی که ازقبل توظیف گردیده اند چک وکنترول شده عوامل عارضه وسیله متذکره را تثبیت واجرااات ذیل را درنظرداشته باشند:

عوارض وسیله متذکره ناشی ازکدام علت بوده است یعنی وسیله متذکره درجریان وظیفه ویا خارج از وظیفه عوارض برداشته است، درصورت که غفلت وظیفوي ثابت شود جنس متذکره تثبیت خساره گردیده وشخص مسئوول آنرا جبران نماید.

آیا مصارف ترمیم وسیله متذکره از50 فیصد تجاوزمینماید یا خیر؟ درصورت که قیمت ترمیم آن از50 فیصد تجاوزنماید قابل ترمیم نمی باشد. با نظرداشت نکات فوق هیت موظف در مورد ترمیم وتبدیلی پرزه جات اقدام می نمانید.
آمرین اعطا بعد ازدرك حقایق وشواهد و نظرهئیت تخنیکی هدایت ترمیم /تبدیل پرزه/ بررسی خساره ازطریق مرجع مربوطه و یا تنزیل کتگوري واسترداد بمنظورجلوگیري ازمصارف بیشتراز50 فیصد قیمت اصلی جنس ابراز نظر میدارند.

ضرورت پرزه جات به اساس فورم 14 از طریق ورکشاپ مرکزي و ساحوي بعد از طی مراحل قانونی از طریق مدیریت عمومی اکمالات ذریعه فورم های 11 و 9 صورت میگیرد البته مصرف پرزه جات به اساس فورم های 63 و 12 بعد از طی مراحل قانونی از جمع معتمد وضع و به خرچ ان مجرا میگردد.

8- صلاحیت های نظارتی ومسئولیت های بخش ورکشاپ ولایات

تحت رهنمود مستقیم مدیریت مخابره و تکنالوژی معلوماتی و پالیسی وپروسیجرهای طرح شده ازطرف مسئوولین مدیریت ورکشاپ که درضمیمه (6) تذکر یافته طرح گردیده باشد مسئوولیت ها و نظارتهای ذیل را بدوش دارد:

- حفظ ومراقبت (ترمیم) وسایل مربوط به بخشهای ارتباطات بدون درنظرداشت قدمه ها بادرنظرداشت اینکه وسایل مربوط به بخش ارتباطات وزارت امورداخله بوده وباید حمایه شوند.
- تنظیم درست ومحافظه مناسب پرزه جات ووسایل مربوط به ترمیمات.
- ارایه نیازمندي های پرزه جات به اساس آسیب پذیري های آن.
- اتخاذ تدابیراحتیاطی وطرزمعقول استفاده از وسایل بخشهای ارتباطی به سطح ولایات.
- وسایل که بعدازطی مراحل اصولی و قانونی غیرقابل ترمیم و یا مصارف بیشتراز50% تثبیت گردد قبل ازاسترداد معلومات ذخیره شده درحافظه ویا ثبت فریکانس آن یا ازطریق خود وسیله یا وسیله دیگرتخلیه شود.

مسئولیت ها

الف – مسئولیت های ریاست عمومی تسهیلات وبخش های ساحوي آن

دراختیارگذاشتن وحفظ ومراقبت تاسیسات (اطاق ها) محلات که کیبل های نوري زیرزمین حفرگردیده ویا درزیرزمین لین دوانی میگردد،کیبل های داخل تعمیرات، آنتن ها ووسایل اخذ وارسال سگنال ها وسویچها(رك)آلماریهای داخل

تعمیرات مختلف مربوط شبکه مرکزي وساحوي رادرنظرگرفته تادرجریان کندن کاریها، بازسازیها ورنگمالی تعمیرات آسیب نبینند.

آسیب وتخریب وسایل وسیستم های مربوطه ارتباطات زیان به تسهیلات دولتی بوده قابل بازرسی وتنبیه مالی میباشد.

بمنظورتهیه انرژي برق نورمال ومموردضرورت شبکه ازطریق برق شبکه شهري ویاجنراتورازطرف انجینران یا مسئوولین تعمیرات طوردوامدارکنترول ومحافظت شودتاباعث شارتی وبروزعوارض در وسایل شبکه نگردد.

تاسیسات (اطاق ها) ازآسیب پذیري طبیعی، برف وباران محافظت شوند و به منظورسرد نگهداشتن سرورها و وسایل ایرکاندیشن (AC)ها ي نصب شده فعال نگهداشته شود.

ب - مسئولیت های ریاست مالی وبودجه وبخش های مربوطه آن

درنظرگرفتن تخصیص کافی بمنظورتهیه وسایل مخابروي، تکنالوژی معلوماتی،حفظ ومراقبت، شبکه و تادیه های آنلاین جوازها (لایسنس ها) سافت ویرهای موردضرورت شبکه.

تهیه دبیت کارت ها(Debit cards)بمنظورتادیه های آنلاین.

ج - مسئولیت های ریاست عمومی پیژنتون ومدیریت های پیژنتون جزوتام ها وادارات

به منظورتقرروجذب افرادمناسب (منسوبین وزارت امورداخله) برای اشغال بستهای مشخص تکنالوژی معلوماتی وشبکه نیازبه یک هماهنگی وارزیابی ازطریق تفاهم با ریاست عمومی مخابره و تکنالوژی معلوماتی دارد تا یک پروسیجر(طرزالعمل)مختصردرزمینه ارزیابی سویه و مناسب بودن افراد به بستهای مشخص ترتیب شده از انحصاربالای اجیران باالمقطع وموقتی جلوگیري شود. بست های مشخص فنی مانند انجینري، مسوولین تخنیکی، مسوولین تکنالوژی معلوماتی، شبکه واستادان طبق پالیسی کادري ریاست عمومی مخابره و تکنالوژی معلوماتی ازطریق اعلانات و رقابت آزاد اکمال گردد.

مصارف وسرمایه گذاري صرف بالای منسوبین وزارت امورداخله صورت گیرد تا مسئوولیت پذیري وحسابدهی بهتر ایجاد شود.

د - مسئولیت های ریاست تنظیم و اداره قوت های پولیس

در هنگام ترتیب تشکیلات جزوتام ها بست های مشخص افسری، ساتنمنی و مامورین ملکی را درنظرداشته باشند تا ازیک طرف در امورمحوله سکتگی رونما نگردیده و ازجانب دیگر محرمیت آن حفظ شده باشد.

ه- مسئولین ها وصلاحیت های نظارتی قوماندانان، آمرین ادارات وجزوتام ها

چون این طرزالعمل بمنظورتنظیم بهترامورارتباطات و تکنالوژی معلوماتی به سطح وزارت امورداخله طرح گردیده تا وظایف روزمره، فوق العاده، اداره منابع معلوماتی وعملیاتهای جزوتام ها به شکل موثر و مناسب آن صورت گیرد که دسترسی به موفیقت های مذکور ازطریق همکاري های همه جانبه، زمینه سازي و رهنمایی های لازم آمرین و قوماندانان حاصل شده می تواند ازتطبیق پروگرامها وشرایط ذیل به سطح جزوتام مربوطه شان کنترول ونظارت مینمایند:

- تطبیق پالیسی های تنظیم وحمایه ارتباطات.

- طرزمعقول استفاده ازوسایل کمپیوتري ومخابروي به سطح اداره مربوطه.
- تنظیم امورحفظ، مراقبت و ترمیم وسایل ارتباطی.
- تطبیق موثرپروگرامهای آموزشی، تخصصی تکنالوژی معلوماتی ومخابره.
- محاسبه درست وموجودي دقیق وسایل، تجهیزات و وسایل ارتباطی.
- حمایت ازپالیسی کادري ریاست عمومی مخابره و تکنالوژی معلوماتی.

احکام متفرقه

مدیریت ویب سایت، رسانه های اجتماعی و دیتابس های داخلی

بمنظور اطلاع رسانی عامه از فعالیت های وزارت امور داخله و قدمه های آن، معلوماتی که از لحاظ محرمیت برای نشر بصورت گسترده از طریق اینترنت مشکلی نداشته باشند و از طرف ریاست ع مخابره برای نشر تایید شده باشد میتواند به نشر برسد.

ویب سایت و شبکه های اجتماعی (فیسبوک، تویتر، گوگل پلس، فلیکر، ساوندکلاود و غیره) وزارت امور داخله و دیگر ویب سایت ها که مربوط وزارت امور داخله می باشد، باید مطابق به شرایط ذیل ویب سایت و شبکه های اجتماعی را مدیریت کنند:

تمام محتویات در ویب سایت و شبکه های اجتماعی باید درست، مرتبط و صحت داشته باشند.

محتویات ویب سایت و دیتابس های داخلی باید در ختم هر سال مرور و بازنگری گردد و معلوماتی که تاریخ اعتبار آن گذشته باید برداشته شود (مثلن بیوگرافی، آدرس شخصی که دیگر در همان موقف یا اداره نیست، یا طرزالعمل ها و پالیسی های ملغی).

نشر اسنادی که به اعتبار وزارت امور داخله لطمه وارد می کند نباید بصورت همگانی به نشر برسد.

معلوماتی که در ویب سایت و دیگر شبکه های اجتماعی آپلود می شود باید از نگاه ساختاری ثابت بوده و یک طرح (فارمت) خاص را تعقیب کند.

سیستم اداره اطلاعات (NIMS)

بمنظور رفع نواقص و کاستی ها در سیستم استخباراتی و کشفی وزارت اموردا‌خله، به همکاری مشاورین بین المللی سیستم اداره اطلاعات (NIMS) شکل گرفت.

مطابق این طرزالعمل تمام ادارات کشفی واستخباراتی وزارت اموردا‌خله میتوانند بمنظور سهولت های کاری که در سیستم وجود دارد طی پیشنهاد عنوانی میام محترم وزارت امور داخله درخواست توسعه سیستم نیمز به کارمندان و قدمه خویش را نمایند.

ازاینکه مدیریت سیستم متذکره به عهده ریاست هدفگیری انت استخبارات میباشد، طبق یک تفاهمنامه حق دسترسی دادن و ایجاد حساب برای کارمندان خویش مطالبه نمایند که البته کنترول اطلاعات ثبت شده مربوط آن اداره میباشد.

برای داشتن حساب کاربری در سیستم نیمز شرایط ذیل حتمی است:

تزکیه امنیتی (پاراگراف بایمتری) کارمند که از لحاظ استخباراتی پروسه را سپری نموده باشد.

کاربر دورهای آموزش نیمز را فرا گرفته باشد (در قوماندانی تعلیم و تربیه، استخبارات و شرکت آدراس)

همه کارمندان به تمام معلومات سیستم اطلاعاتی ملی نیمز دسترسی نخواهند داشت و صلاحیت ها از طریق امرین بخش ها تعیین خواهد شد.

سیستم نیمز برای تمام وزارت امور داخله ایجاد شده است که برای هر ریاست در سیستم نیمز دیتابیس های جداگانه به اساس مقررات در چوکات کاری شان ایجاد شده است. برای دسترسی باید هر ریاست بطور جداگانه در دیتابیس مربوطه خویش صلاحیت کاری و

حدود دسترسی کارمندان خویش را مشخص سازد.

قبل از اینکه کارمندان صلاحیت دسترسی نمیز را حاصل نمایند بصورت رسمی از طریق اداره مربوط معرفی و کاپی کارت هویت و فورم که ازطرف اداره مربوط تصدیق گردیده باشد ارایه بدارد.

تلاش جهت دسترسی به سطح بلند تر نسبت به سطح اجازه داده شده، سو استفاده از رمزهای ورودی، تغییر بست شخص ذیصلاح باعث می شود تا کارمند دیگر به سیستم نیمز دسترسی نداشته باشد.

سیستم مدیریت معلومات صحی (HMIS)

این سیستم بمنظور سهولت بخشیدن فعالیت های ریاست صحیه انشکاف داده شده است و این سیستم دارای قابلیت های ذیل می باشد:

ثبت بیماران در کلینیک و شفاخانه ها که تمام پروسه از ثبیت نام، جریان تداوی و رخصت شدن مریض تمام در این سیستم انجام می شود.

تمام بخش ها و بستر ها دارای شماره منحصر به فرد در سیستم هستند که مدیریت شفاخانه یا کیلنیک و جریان تداوی مریض را سهولت می بخشد.

مدیریت دواخانه – می توان تعداد دواهای فراهم شده را برای هر مریض کنترل کرد و نیز میتوان موجودی دواها را در دواخانه حساب کرد. تاریخ انفضا هر دوا در سیستم ثبت میشود و شخص مسوول را از این امر با خبر می سازد.

مدیریت لابراتوار – تمام تست های گرفته شده از بیمار در سیستم ثبت می شود و با داکتر معالج از طریق سیستم شریک ساخته می شود.

ضبط الکترونیکی پیشینه پزشکی بیمار در سیستم که داکتر را برای درمان بیمار در آینده کمک می کند.

بمنظور استفاده بهینه از این سیستم طرزالعمل هایی باید انکشاف یابد تا منسوبین ذیدخل با قابلیت های سیستم آشنا شوند و روزمره از آن کار بگیرند.

سیستم مدیریت تفتیش (Case Managent system)

این سیستم تمام موارد مربوط به ریاست عمومی تفتیش (OIG) را مدیریت می کند و وضعیت پرونده ها را بررسی می کند. این سیستم ریاست عمومی تفتیش را قادر می سازد تا کنترل بروی تمام موارد داشته باشند; از قبیل وضعیت مورد، مورد نزد کدام فرد در حال انتظار است، و پیشرفت کار. این سیستم باعث بوجود آمدن شفافیت و حسابدهی در ریاست عمومی تفتیش می شود. بمنظور استفاده بهینه از این سیستم طرزالعمل هایی باید انکشاف یابد تا منسوبین ذیدخل با قابلیت های سیستم آشنا شوند و روزمره از آن کار بگیرند.

سیستم تصویب پلان سالانه تدارکاتی (Annual Procurement Plan Approval System)

این سیستم به ۱۴ ریاست واحد بودجوی این امکان را می دهد تا پلان های تدارکاتی خویش را از طریق یک طرح (فارمت) واحد تهیه و با یکدیگر شریک بسازند. پلان های تدارکاتی توسط سیستم توحید شده و ریاست تدارکات را قادر می سازد تا پلان توحید شده را مرور و بازنگری کند. سیستم امکان آن را می دهد تا پلان تدارکاتی توحید شده با رهبریت وزارت امور

داخله شریک شود و در صورت تغییر در پلان، سیستم این اجازه را می دهد تا پلان نیز بروزرسانی شود. بمنظور استفاده بهینه از این سیستم طرزالعمل هایی باید انکشاف یابد تا منسوبین ذیدخل با قابلیت های سیستم آشنا شوند و روزمره از آن کار بگیرند.

سیستم مدیریت شهدا و مجروحین

این سیستم تمامی منسوبین وزارت امور داخله را در یک سیستم واحد ثبت می کند، اطلاعات کاملی از شهدا و ورثه آنانذر سیستم ذخیره می شود. این سیستم تمام پرداختی ها که شامیل فامیل شهیدا و زخمی ها می شود را در ثبت می کند. بمنظور استفاده بهینه از این سیستم طرزالعمل هایی باید انکشاف یابد تا منسوبین ذیدخل با قابلیت های سیستم آشنا شوند و روزمره از آن کار بگیرند.

سیستم مدیریت اسناد (Document Mangement System)

این سیستم برای ریاست عمومی پلان و پالیسی طرح شده است و این امکان را می دهد تا پالیسی ها، طرزالعمل ها و دیگر اسناد در یک محل نگهداری شود. از قابلیت های این سیستم میتوان جستجوی محتوا و دسترسی بر اساس کاربر را نام گرفت. بمنظور استفاده بهینه از این سیستم طرزالعمل هایی باید انکشاف یابد تا منسوبین ذیدخل با قابلیت های سیستم آشنا شوند و روزمره از آن کار بگیرند.

دفتر مقام – این سیستم توسط دفتر مقام وزیر بمنظور مدیریت اسناد، پردازش اسناد / جمع آوری عرایض، جستجوی محتوا در سند، حفظ اسناد استفاده می شود.

مالی و بودجه- این سیستم توسط دفتر مقام وزیر بمنظور مدیریت اسناد، پردازش اسناد / جمع آوری عرایض، جستجوی محتوا در سند، حفظ اسناد استفاده می شود.

سیستم مدیریت شکایت (Complaint Management System)

این سیستم پنجره ای را برای همه شکایت کنندگان فراهم می کند تا شکایات خود را از طریق یک سیستم متمرکز ثبت کنند، این سیستم شکایت ثبت شده را به دفتر شکایت که تحت دفتر مقام کار می کند هدایت می کند بدون آنکه هویت شخص شاکی آشکار شود. سیستم یک شماره شکایت منحصر به فرد برای شکایت ایجاد می کند و از طریق آن تعداد شکایت کننده می تواند وضعیت شکایت خود را ببیند، اداره شکایت تحت دفتر مقام می تواند شکایت را به اداره مربوطه از طریق سیستم برای تحقیقات بیشتر بفرستد. ریاست مربوطه جواب شکایات به اداره شکایت تحت دفتر مقام بعد از اتمام تحقیقات فرستاده می تواند.

سیستم مدیریت کمک ها

ریاست هماهنگی های بین المللی

در سطح استراتژیک، سیستم مدیریت کمک ها در همخوانی با استراتیژی کمک های دریافتی به وزارت امور داخله دارد. سیستم بمنظور مدیریت کمک های مالی تمویل کنندگان توسعه یافته است. بطور عمده قابلیت های سیستم به چند بخش تقسیم می شود:

با گزارشات تولید شده از سیستم می توان رویکرد مبتنی بر شواهد را در وزارت امور داخله ترویج ساخت.

تخصیص، مشارکت و کمک به نظارت از برنامه های وزات امور داخله.

اطلاع رسانی در قسمت مالی و بودجوی

ایجاد هماهنگی بین منابع تمویل کننده خارجی با اولویت های وزرات امور داخله و پرکردن شکاف های مالی.

ثبت تمام منابع مالی خارجی به وزارت امور داخله

ترویج ساخت بودجه بر اساس برنامه

نشر و بازنگری طرزالعمل

این طرزالعمل به اساس مکتوب 1028 مورخ 1396/7/26 ریاست محترم ع دفتر معینیت ارشد امور امنیتی توسط گروپ کاری مرور پالیسی ریاست ع مخابره و تکنالوجی معلوماتی طی جلسات متعدد ترتیب گردیده و با تشکر از گروپ کاری و همکاران ریاست ع پلان و پالیسی خصوصاً مشاوریت مقام که در تصحیح متن قبل از منظوری جهت منظوری به مقام محترم تشریح است که این طرزالعمل بعد از منظوری وزیر امور داخله به تمام ادارات مربوط رسماً ارسال میگردد همچنان از طریق سایت شیرپاینت (http://moinocsc03/sites/policy/_layouts/15/start.aspx) نیز به دست نشر سپرده میشود.

همچنان این طرزالعمل بعد ازتاریخ منظوري و سپري شدن مدت یکسال توسط ریاست عمومی پلان و پالیسی مرورمیشود. درجریان یکسال به اساس نیازمندي ها وتوسعه وسایل وتجهیزات مخابروي وسیستم تکنالوژی، پروسیجرهای لازم بشکل ضمیمه به این طرزالعمل الحاق شده می تواند.

نظارت و ارزیابی:

ریاست عمومی مخابره و تکنالوژی معلوماتی معینیت ارشد امور امنیتی و ادارات ذیربط، پالیسی پلان های تطبیقی را مطابق به مکلفیت هایشان ترتیب و در ظرف یک ماه بعد از منظوری و تکثیر پالیسی به ریاست عمومی پلان و پالیسی ارسال نمایند. تا هنگام نظارت و بررسی از تطبیق پالیسی توسط گروپ های نظارتی ریاست عمومی نظارت و ارزیابی معینیت پالیسی و استراتیژی اقدام صورت گیرد.

محمد رضا کاتب

ریاست عمومی پلان وپالیسی

فورم ثبت ورودی و خروجی کارمندان به دیتاسنتر									
شماره	نام	نام پدر	شماره کارت هویت	شرح دلیل بازدید از دیتاسنتر	تاریخ	زمان دخول	زمان خروج	امضاء	ملاحظات
۱									
۲									
۳									
۴									
۵									
۶									
۷									
۸									
۹									
۱۰									

ضمیمه 2: فورم توافق نامه کاربر(User Agreement form)

نام و تخلص:..... نام پدر:..... رتبه/بست:..... نام کاربر: .....

ولایت:..... آمریت:..... مدیریت:..... ریاست:..... تیلفون شخصی:.....

نام کمپیوتر: .....

رهنود های ذیل در مورد استفاده مجاز و درست از وسایل تکنالوژی معلوماتی وزارت داخله میباشد.

- استفاده از خدمات انترنتی شبکه (وزارت داخله) تنها در کار های رسمی صورت می گیرد.
- اگر از حساب دسترسی خود بیش از 60 روز استفاده نکنم، حسابم بسته(Disable) خواهد شد.
- از نصب کمپیوتر ها و وسایل دیگر غیر دولتی در شبکه خود داری می کنم.
- از تغییر دادن رمز ورودی (رمز عبوری) ادمنستریتور محلی خود داری نموده و به هیچ صورت سیستم کمپیوتر را، که "ویندوز" است، به سیستم دیگر تبدیل نخواهم نمود.
- از نصب نرم افزار (سافت ویر) هایی که از سوی دیپارتمنت آی سی تی منظور نگردیده باشد، خود داری می ورزم.
- از دست زدن به اعمال غیر قانونی و هر عملی که به اعتبار وزارت داخله ضربه بزند خود داری مینمایم.
- استفاده از امکانات آی تی به هدف های تجارتی و فعالیت های انتفاعی و در پشتیبانی از استخدام در خارج (ازوزارت) و یا فعالیت های تجارتی(مثلاً، مشوره در بدل پول، فروش و یا اداره معاملات تجارتی و فروش اشیاء و خدمات) خود داری می کنم.
- از هر نوع استفاده شخصی که باعث ازدحام، تاخیر و یا اخلال خدمات در سیستم و وسایل دولتی شود خود داری می ورزم. به گونه مثال، از ارسال کارت ها تبریکی، ضمیمه ساختن (اتچمنت)، فایل های ویدیویی و صوتی و فایل های بزرگ دیگری که سطح فعالیت تمام شبکه را پائین می آورد خود داری می کنم. استفاده ازهر گونه سافت ویرهای که باعث بطی شدن فعالیت تمام شبکه می گردد استفاده نادرست محسوب میگردد.
- از دست زدن به فعالیت هایی که باعث آسیب رسانیدن به مصئونیت کمپیوتر های دولتی وصل شده به شبکه خودداری می نمایم. رمز دسترسی به حساب را به کاربر های دیگر افشاء ننموده و با آنها شریک نمی نمایم.
- از استفاده شبکه وزارت داخله به منظور نقطه آغاز برای دستیابی غیر قانونی به شبکه های دیگر خود داری می کنم.
- از ایجاد، نقل، ارسال و ارسال مجدد مکاتیب زنجیره ای و یا ارسال غیر مجاز مکاتیب به آدرس های متعدد بدون در نظر داشت موضوع آنها خود داری می ورزم.
- اشتغال در فعالیت های جمع آوری اعانه، تائید از محصولات و خدمات، یا اشتراک در فعالیت های لابی (فعالیت برای جلب نظر قانونسازان به نفع یک قضیه....) و اشتغال در فعالیت های سیاسی مجاز نیست.

دیگران را به خاطر وابستگی نژادی، دینی و مذهبی، رنگ پوست، جنسیت، معلولیت و مورد تمسخر قرار دهد، می گردد.

- ایجاد، پیاده کردن (دونلود)، دیدن، حفظ، نقل گرفتن و ارسال مطالب برهنه جنسی و یا مطالب دیگری که با تمایلات جنسی رابطه دارد، ممنوع است.
- ایجاد، پیاده کردن (دونلود)، دیدن، حفظ،، نقل گرفتن و ارسال مطالب در مورد قمار، سلاح های غیر قانونی، فعالیت های تروریستی و فعالیت های دیگر غیر قانونی و فعالیت های ممنوعه، مجاز نمی باشد.

من به این مطلب آگاهی کامل دارم که کمپیوتر های دولتی تنها به منظور استفاده رسمی اند. دولت به خاطر استفاده من از کمپیوتر های دولتی به صورت مستقیم و یا غیر مستقیم پول نمی گیرد. اگر برای من اجازه دسترسی به انترنت داده شود تنها با استفاده از کمپیوتر دولتی این کار را می کنم. داخل شدن به انترنت در انترانت با استفاده از کمپیوتر شخصی مجاز نیست.

من می دانم که وزارت داخله هر زمانی که بخواهد می تواند استفادة من از کمپیوتر دولتی را زیر نظر داشته باشد. هر نوع استفاده نا درست منجر به قطع استفاده از این خدمات گردیده و یا اجراات اداری وزارت در قبال خواهد داشت. من به تحت نظر قرار گرفتن در زمان استفاده از کمپیوتر ها در شبکة دولتی موافق هستم.

اینجانب که شهرت مکملم در فوق ذکر گردیده با تمامی رهنمود ها و قوانین استفاده درست از وسایل تکنالوژی معلوماتی وزارت امور داخله موافق و متعهد میباشم.

امضا و تاریخ: _____ **امضاء امر مخابره مدیریت مربوطه:** _____

امضا و تصدیق مدیریت عمومی شبکه ناک:

ضمیمه 3: فورم دسترسی به وسایل جانبی

نام و تخلص: ..... نام پدر:..... رتبه/بست:..... نام کاربر:.....

ولایت:..... آمریت:..... مدیریت:..... ریاست:..... تیلفون شخصی:..... .....

1. چرا شما میخواهد که به وسایل جانبی دسترسی داشته باشید دلیل آنرا توضیح دهید؟
2. آیا در مدیریت شما شخص دیگر به وسایل جانبی دسترسی دارد یا خیر؟
اینجانب که شهرتم در فوق ذکر گردیده نظر به دلایل فوق دسترسی به وسایل جانبی از طریق شبکه وزارت امور داخله را ضرورت دارم و مسؤلیت هر نوع حمله یا حادثه را به شبکه وزارت اموردااخله به صورت خواسته یا ناخواسته از ناحیه خویش را میداشته باشم. نام..... امضا، تاریخ و مهر اداره.....
قسمت ذیل صرف توسط اداره مربوطه خانه پوری میگردد.(مدیریت مربوطه)
اینجانب.....(بست و وظیفه)..... موافقم که شخص فوق الذکر دسترسی به وسایل جانبی از طریق شبکه وزارت امور داخله را ضرورت داشته، مسؤل و جوابگوی هر نوع مشکلات و حادثات که از طریق شخص فوق الذکر رخ میدهد میباشم. امضا، تاریخ و مهر اداره.....
قسمت ذیل صرف توسط مسئولین مدیریت عمومی ارتباطات استراتیژیک خانه پوری میگردد.
مدیریت فوق الذکر جمله ( ) استفاده کننده(User) دارد که از جمله ( ) استفاده کننده دسترسی به وسایل جانبی آن فعال گردیده معلومات داده شده در زمینه آنچه هدایت میفرمایند موجب تعمیل است. مسئول تیم حمایوی ..... مسئول سیستم.....مدیر سرورها .....مدیرع ارتباطات ستراتیژیک.....
قسمت ذیل صرف توسط ریاست مخابره و تکنالوژی معلوماتی تصدیق میگردد.
در صورت قبول نمودن مسؤلیت های بعدی توسط اداره و نبود موانع امنیتی دسترسی به وسایل جانبی را برایشان فراهم سازید. ریاست عمومی مخابره و تکنالوژی معلوماتی امضا و تاریخ و مهر اداره.....

ضمیمه 4: فورم دسترسی کامل انترنت(Full Access)

نام و تخلص: ..... نام پدر:..... رتبه/بست:..... تیلفون شعبه:.....

ولایت:..... آمریت:..... مدیریت:..... ریاست:..... تیلفون شخصی:.....

نام کاربر(User Name): ..... نام کمپیوتر(Computer Name):..... آدرس فیزیکی(MAC):.....

1.دلایل ضرورت به دسترسی کامل به انترنت را واضح سازید؟
2. شما به کدام سایت ها ضرورت دارید که دسترسی آن برایتان در حالت فعلی داده نشده است در ذیل لیست نمایید؟
اینجانب که شهرتم در فوق ذکر گردیده نظر به دلایل فوق دسترسی کامل به انترنت از طریق شبکه وزارت امور داخله را ضرورت دارم و مسؤلیت هر نوع حمله یا حادثه را به شبکه وزارت اموردخله به صورت خواسته یا ناخواسته شخصا متقبل میگردم. امضا، تاریخ.....
تضمین کننده: اسم: رتبه: وظیفه: اداره مربوطه:
اینجانب که شهرتم در فوق ذکر گردیده مسؤل و جوابگوی هر نوع مشکلات و حادثات که از طریق شخص فوق الذکر رخ میدهد را میباشم. امضا، تاریخ و مهر اداره.....
قسمت ذیل صرف توسط ریاست مخابره و تکنالوژی معلوماتی تصدیق میگردد.
در صورت قبول نمودن مسؤلیت های بعدی توسط اداره و نبود موانع امنیتی دسترسی به منابع انترنت را برایشان فراهم سازید. امضا و تاریخ و مهر اداره..... ریاست عمومی مخابره و تکنالوژی معلومات

ضمیمه 5: جدول مسئولیت و نظارت وظایف اساسی ریاست عمومی مخابره و تکنالوژی معلوماتی

شماره	نوع صلاحیت نظارت مسوولیت	ریاست عمومی مخابره و تکنالوژی معلوماتی و معاون آن	مدیریت ع شبکه و تکنالوژی	مدیریت دیتابس ها	مدیریت سرورها	مدیریت دیتاسنتر	مدیریت توسعه شبکه	مدیریت عمومی مراکز مخابره	مدیریت اداره و تنظیم فریکونسی	مدیریت پیام ها و محرم سازی
۱	اداره و رهبری تمام بخش های مربوط به ارتباطات و منابع معلوماتی به سطح وزارت امور داخله	●								
۲	تامین ارتباطات استراتیژیک، اداره، تنظیم و فعال نگهداشتن شبکه		●							
۳	حمایه، توسعه و تنظیم دیتابس ها			●						
۴	تنظیم و حمایه سرور های شبکه مرکزی و ساحوی				●					
۵	تنظیم و ذخیره معلومات (بک آپ)					●				
۶	حفظ، مراقبت و توسعه شبکه						●			
۷	تامین ارتباطات تکنیکی و اخذ و ارسال پیام های مخابروی							●		
۸	تنظیم و اداره فریکانس ها								●	
۹	اخذ و ارسال پیام های شفری									●

ضمیمه 6: بخش نظارت و مسئولیت ها وظایف حمایوی ریاست عمومی مخابره و تکنالوژی معلوماتی

شماره	صلاحیت نظارتی و مسوولیت ها	مدیریت عمومی تعلیم و تربیه	مدیریت عمومی اکمالات	مدیریت ورکشاپ	مدیریت تخصیص و بودجه	مدیریت پیژتون
۱	طرح و تطبیق برنامه های آموزشی کمپیوتر و مخابره	●				
۲	اکمال و توزیع وسایل کمپیوتری و مخابروی		●			
۳	حفظ و مراقبت (ترمیم) وسایل کمپیوتری و مخابروی			●		
۴	بخش بودجه و تخصیص				●	
۵	ساختار بخش های ارتباطات و انتخابات افراد واجد شرایط					●

جمهوری اسلامی افغانستان

وزارت امور داخله

معینیت ارشد امور امنیتی

ریاست عمومی مخابره و تکناروژی معلوماتی

Application Form ___ فورم درخواستی 201 / /

Name: اسم:		Last Name: تخلص:	
Personal Phone # شماره تلیفون شخصی		Office Phone #: شماره تلیفون دفتر:	
Email Address of the User : آدرس ایمیل کاربر :			
Company or Ministry: شرکت یا وزارت :		Department: دیپارتمنت :	
Name of Company or Ministry Supervisor اسم سوپروایزر شرکت یا وزارت :		Supervisor's Phone Number شماره تلیفون سوپروایزر :	
Supervisor's Email address : آدرس ایمیل سوپروایزر :			
Current username of the MOI privileged user account or 3rd party privileged user account which will be used on the network: حساب فعلی کاربر با صلاحیت وزارت داخله یا کاربر حساب شرکت ثالث که در شبکه استفاده خواهد شد:			
Does the user have or has ever had a user account or privileged user account on the MOI network at any time? آیا کاربر دارای حساب کاربر با صلاحیت وزارت داخله می باشد یا کدام وقت بوده؟			☐ Yes / بلی ☐ No / نخیر
If so what accounts did they have access to? اگر جواب مثبت است، به کدام حساب ها دسترسی داشته است؟			
User Computer Ownership: مالکیت کمپیوتر کاربر	☐ MOI ICT / ریاست مخابره	☐ Company / شرکت	Personal / شخصی ☐
	Other / دیگر:		
Computer Name which will be used to remotely connect to MOI resources: نام کمپیوتر که برای دسترسی از راه دور برای وصل شدند به منابع وزارت داخله استفاده میشود:			
IP Address, or make note if IP address is assigned dynamically. www.whatismyipaddress.com آی-پی ادرس، یا اگر بصورت دینامیک است یادداشت دهید			
Computer MAC Address (aabb.ccdd.eeff): مک ادرس کمپیوتر:			
Along with this form attach a signed memorandum how the user will allow MOI provided Anti-Virus and security patches on user's computer and authorize a full rootkit memory and system scan before access to MOI resources. And the user will allow the removal of any software infected with malicious virus, Trojans, and worms that are directly installed on the computer or attached to pirated software before connecting to the network. The MOI is not responsible for disabling or removing pirated software during malicious content cleanup. یک یاد داشت امضا شده را ضمیمه با این فورمه ارایه نمایید که چگونه کاربر اجازه خواهد داد که MOI Anti-Virus و patch های امنیتی را بر روی دستگاه منبع ارسال کند و قبل از دسترسی سکن کامل حافظه rootkit و اسکن سیستم را تأیید کند. و کاربر اجازه حذف هر نرم			

افزاری را که آلوده به ویروس مخرب، تروجان ها و ورم هایی است که به طور مستقیم بر روی کامپیوتر نصب شده اند یا به نرم افزارهای جاسوسی متصل می شوند قبل از اتصال به شبکه اجازه می دهد. وزارت داخله مسئول از بین بردن نرم افزارهای جاسوسی در پاک کردن محتوای مخرب نیست.
Provide detailed technical justification for VPN access request. لطفا توجیه تخنیکی برای درخواست دسترسی وی-پی-ان ارایه نمایید.
How long is VPN access required? Note: Maximum allowed access is 30 days. For requests up to 1 year, business justification needs to be provided and approved by MOI ICT Leadership. برای چه مدت دسترسی وی-پی-ان نیاز است؟ نوت: حد اعظمی مجاز 30 روز میباشد. برای درخواست تا یک سال، نیاز به توجیه تجارتی و تایید رهبری ریاست مخابره وزارت داخله میباشد.
Provide a signed memorandum by the user that they agree to only access the resources identified in this request and not attempt to access any other resources. They additionally agree to have all traffic monitored while on the network. یک یادداشت امضا شده توسط کاربر ارایه نمایید که آنها فقط به دسترسی به منابع مشخص شده در این درخواست موافقت مینمایند و نه برای تلاش برای دسترسی به هر گونه منابع دیگر. علاوه بر این موافقت مینمایند تا تمام ترافیک تا وقتی در نیتورک هستند زیر نظارت خواهد بود.
What specific resource within hosting network is required (i.e., Information System X with this IP address and this TCP port. Remote users will not have direct Internet access through the *MOI and will only be able to access the internal resources requested. If only a specific port access is needed, for example http access to a specific URL or IP address, the policy will provide that minimum access to support the work. چه منابع خاصی در داخل شبکه میزبانی مورد نیاز است (به عنوان مثال، سیستم اطلاعاتی X با این آدرس IP و این پورت TCP .)کاربران از راه دور دسترسی مستقیم از طریق MOIبه اینترنت ندارند و تنها قادر به دسترسی به منابع داخلی مورد درخواست است. اگر فقط دسترسی به پورت خاص مورد نیاز است، به عنوان مثال دسترسی http به URL خاص یا آدرسIP ، پالیسی حداقل دسترسی را برای پشتیبانی از کار فراهم می کند.

Applicant Signature: محل امضاۀ درخواست کننده	Supervisor / Office Verification: محل تاییدی رییس / دفتر

Note this application needs to have the two referenced Memos to be complete. Only when complete will it be accepted. Please attach other documents and papers supporting your application with this form.

این درخواستی نیاز به دو یادداشت مرجع دارد که باید کامل شود .تنها وقتی پذیرفته میشود که تکمیل شده باشد. لطفا اسناد و مدارک دیگر که از این فرم یا درخواست شما پشتیبانی می کنند، ضمیمه کنید.

ضمیمه 8: پلان تطبیقی طرزالعمل مخابره و تکنالوژی معلوماتی

هدف طرزالعمل:																
محصول:																
قیمت تخمینی:																
شماره	فعالیت های عمده	فعالیت های فرعی	شاخص	مبدأ		زمان اجرأ				اداره مسؤل	اداره همکار	فیصدی پیشرفت			
				1397	1398	1	2	3	4			ربع اول	ربع دوم	ربع سوم	ربع چهارم
1															
۲															

قرار شرح فوق پلان هذا ترتیب وقابل تطبیق است.

امضا آمر ذیصلاح

متصدی پالیسی/طرزالعمل:

متصدی طرزالعمل به اساس دایرکتیف تدوین طرزالعمل افسر وزارت امور داخله که مسولیت های اسنادی طرزالعمل را اولویت دهی و حمایه نموده و از تطبیق، نظارت، گزارش دهی و مرور آن اطمینان حاصل مینماید.

توظیف متصدی طرزالعمل یا گروپ کاری برای هریک از اسناد پالیسی و طرزالعمل وزارت امور داخله از صلاحیت های ریاست عمومی پلان و پالیسی، معینیت پالیسی و استراتیژی است.

متصدی طرزالعمل مسولیت دارد تا روند تکثیر و تطبیق طرزالعمل ها را از قدمه استراتیژیک به قدمه های اوپراتیفی یا تطبیقی پیگیری نماید.

1) مرجع ارسالی طرزالعمل و تاریخ مواصلت ان

این ستون توسط دریافت کننده طرزالعمل (آن شخصی که غرض تطبیق طرزالعمل در اداره توظیف است- ستون شماره 3) با شرح جزئیات صادر کننده تکمیل گردد، مانند : کی طرزالعمل را صادر نمود و تاریخ مواصلت آن.

2) مرجع تطبیق کننده

در این ستون توسط دریافت کننده، قدمه سطح استراتیژیک وزارت امور داخله که مکلف به تطبیق طرزالعمل است درج میگردد، مانند : معینیت، ریاست عمومی مستقل.

3) اسم و رتبه شخص موظف

این ستون با شرح جزئیات پیرامون شخص موظف تطبیق طرزالعمل تکمیل میگردد. این شخص مربوط به تشکیل مرجع تطبیق کننده باید باشد(ستون شماره.2). از طرف مقام ذیصلاح مرجع تطبیق کننده می تواند با درنظرداشت مسوولیت وظیفوی ریاست دفتر توظیف گردد.

4) فعالیت ها در رابطه به تطبیق طرزالعمل

تمام فعالیت های که در رابطه به تطبیق طرزالعمل باید صورت گیرد درین ستون درج میشود، مانند: تکثیر طرزالعمل به قدمه های تحت اثر، استخراج وظایف و مسوولیت ها از متن طرزالعمل (تحلیل و تجزیه طرزالعمل که شامل پلان نمیگردد)، تدویر جلسه یا سمینار در رابطه به اگاهی دهی محتویات طرزالعمل.

طرزالعمل برای مسولین بخش ها، هدایت در رابطه به تطبیق و عملی نمودن سیستم جدیدی که متن طرزالعمل از آن تذکر بعمل امده است، تطبیق و عملی نمودن فورمه ها، فارمت و ضمایم جدید، همچنان در حالتی که تطبیق طرزالعمل به کدام بخش مشخص به صورت اختصاصی ربط داشته باشد توظیف همان بخش درین ستون با جزئیات مسولیت های آن.

موعد اجرا

درین ستون مشخص میگردد که با در نظرداشت امکانات و منابع موجوده وظایف و مسولیت های مندرج ستون (4) در کدام قید زمانی باید عملی شود.

5) قدمه تطبیق کننده

درین ستون قدمه مشخص که مسولیت تطبیق وظایف و مسولیت های مندرج ستون (4) به عهده آن میباشد درج میگردد. در صورتیکه وظایف و مسولیت ها به تمام قدمه های تحت اثر ربط داشته باشد درین ستون بصورت عمومی کلمه "تمام قدمه ها" تحریر میشود.

6) معیاد ارایه معلومات از صورت تطبیق به متصدی

درین ستون توسط مرجع تطبیق کننده طرزالعمل معیاد ارایه معلومات از توسعهات بعدی پروسه تکثیر وتطبیق طرزالعمل به متصدی طرزالعمل جهت اطمینان از اینکه طرزالعمل در مسیر تطبیق قرار گرفته مشخص میگردد.

خاطره:

بعد از منظوری این رهنمود، پیرامون استخراج وظایف و مسولیت ها از متن طرزالعمل، نحوه استفاده از پلان تطبیقی و کار عملی بالای ترتیب پلان تطبیقی به سطح قدمه های استراتیژیک در مرکز و قدمه های اوپراتیفی و تطبیقی در مرکز و ولایت، سیمینار های آموزشی توسط مربیون ریاست عمومی پلان و پالیسی و همکاران بین المللی دایر می گردد.

قرار شرح فوق رهنمود هذا ترتیب و جهت منظوری تقدیم است.

ریاست عمومی پلان و پالیسی