لایحه وظایف پست‌های خدمات ملکی

معلومات کلی پست

شماره اعلان پست:	
عنوان وظیفه:	آمر انکشاف پالیسی و استندرد های سایبری
بست:	۳
وزارت یا اداره:	مخابرات وتکنالوژی معلوماتی
بخش مربوطه:	ریاست امنیت سایبری
موقعیت پست:	مرکز
تعداد پست:	(۱)
گزارشده به:	ریاست امنیت سایبری
گزارش‌گیر از:	کارمندان تحت اثر
کد:	
تاریخ بازنگری:	۱۴۰۱/۵/۳

هدف وظیفه: مطالعه، تحقیق، ایجاد و انکشاف پالیسی های امنیت سایبری داخلی و ملی در مطابقت به استندرد های بین المللی، هماهنگی، تحقیق، حصول اطمینان از تطبیق موثر قوانین، پالیسی ها، طرزالعمل ها

صلاحیت و مسئولیت های وظیفوی:

وظایف تخصصی

۱. تهیه/انکشاف پالیسی ها و استندرد های تکنالوژی معلوماتی و امنیت سایبری مطابق استندرد های ISO/IEC 27001-2، COBIT,ISMS، ISACA و NIST و سایر استندرد های بین المللی.
۲. آموزش تیم انکشاف پالیسی در زمینه تحقیق، تحلیل و ارزیابی نیازمندی، انکشاف پالیسی ها و قوانین امنیت سایبری.
۳. ترتیب پلان موثر و استفاده از استندرد های ISO 27002 security policy، COBIT و NIST و سایر استندرد های امنیت سایبری به منظور رشد سطح آگاهی امنیت سایبری کارمندان ادارات دولتی و شهروندان افغانستان.
۴. حصول اطمینان از پروسه تحقیق، انکشاف پالیسی ها و قوانین امنیت سایبری و اولویت بندی در ارائه گزارش به مقامات ذیصلاح.
۵. تحقیق وفراهم آوری موضوعات جدید و عمده از ستندرد ها وپالیسی های جهانی در راستای امنیت سایبری جهت غنامندی قوانین موجودهء وزارت مخابرات و تکنالوژی معلوماتی.
۶. نظارت از تحقیقات منظم در مورد ستندرد های جهانی مانند ISO/IEC 27701, BS 31111, ISO/IEC 27034, ISO/IEC 27017,BS 7799-3 جهت ارائه مشوره های تخنیکی و انکشاف قوانین و پالیسی های امنیت سایبری کشور.
۷. مطالعه قوانین و مدل های امنیت سایبری کشور های پیشرفته ، تهیه و انکشاف پالیسی ها و استندرد های تکنالوژی معلوماتی و امنیت سایبری مطابق استندرد های ISO/IEC 27001-2, COBIT,ISMS، ISACA و NIST و سایر استندرد های بین المللی.

۸. ارزیابی نیازمندی وزارت مخابرات و سایر ادارات در قسمت ایجاد پالیسی و استندرد ها امنیت سایبری.
۹. ایجاد پلان های کاری و عملیاتی جهت انکشاف پالیسی ها، طرزالعمل ها و رهنمود های امنیت سایبری.
۱۰. نظارت از تحقیق و تحلیل تهدیدات سایبری و ارایه رهنمود های محافظتی جهت آگاهی دهی عامه و درج آن در پلتفورم آگاهی دهی .
۱۱. تحقیق و اطلاع رسانی آسیب پذیری های جدید امنیتی و نشر قوانین و پالیسی های امنیت و جرایم سایبری کشور.

وظایف مدیریتی:

۱. ترتیب پلان کاری ماهوار، ربعوار و سالانه در مطابقت با پلان عمومی، بمنظور رسیدن به اهداف تعیین شده وزارت؛
۲. ارائه گزارش ماهوار، ربعوار، سالانه و عندالضرورت از فعالیت ها و دست آورد های مربوطه، بمنظور مطلع ساختن رهبری وزارت/اداره .
۳. ترتیب راپور انکشاف پالیسی ها، تطبیق استندرد های امنیت سایبری در زیربنا های تکنالوژی معلوماتی.
۴. اجرای سایر وظایف که از طرف مقامات ذیصلاح مطابق قوانین، مقررات و اهداف وزارت مربوطه سپرده میشود.

وظایف هماهنگی

۱. همکاری تخنیکی در انکشاف قوانین و طرزالعمل های فعلی امنیت سایبری مطابق قوانین نافذه کشور با سایر ادارات.
۲. هماهنگی با ادارات و کشور های منطقوی و بین المللی جهت ارتقای ظرفیت و دریافت راهکار های جدید در زمینه انکشاف پالیسی ها و طرزالعمل ها.
۳. همکاری در زمینه ترتیب و انکشاف استراتیژی امنیت سایبری و قوانین سایبری با سکتور دولتی و خصوصی.
۴. همکاری در ایجاد پالیسی ها و استندرد ها با سایر بخش های ریاست عمومی زیربنا های تکنالوژی معلوماتی .
۵. هماهنگی با ادارات جهت مشوره دهی و نظر خواهی در زمینه انکشاف قوانین امنیت سایبری و پالیسی ها.
۶. هماهنگی نزدیک با کمیته های انکشاف قوانین و پالیسی ها با ادارات عدلی و قضایی در زمینه های ایجاد، انکشاف و تصحیح قوانین به اساس نیازمندی داخلی و بین المللی .

.....

(شرایط استخدام (سطح تحصیل و تجربه کاری):

- این لایحهٔ وظایف با در نظر داشت مواد ۷، ۸و ۳۴ قانون کارکنان خدمات ملکی با حد اقل شرایط و معیارهای ذیل ترتیب گردیده است:
- داشتن حداقل سند تحصیلی لیسانس در یکی از رشته های: کمپیوتر ساینس ، تکنالوژی معلوماتی و سایبر سکیورتی و سایر رشته های مرتبط و به درجه تحصیلی بالاتر در رشته های متذکره ارجحیت داده میشود.
- تجربه کاری مرتبط (مدیریتی مشابه ویا تخصصی امور تکنالوجی معلوماتی)ویا سایر موارد مندرج اهداف و مسولیت های وظیفوی این بست)حد اقل ۳ سال برای لیسانس، ۱ یک سال برای ماستر.
- تسلط به یکی از زبان های رسمی(پشتو و یا دری) و آشنایی (تحریر و تکلم) با زبان انگلیسی؛
- مهارت های مسلکی:

a. مهارت و توانمندی عالی در ساختن پلان و پالیسی مطابق استندرد های بین المللی
b. آشنایی با روش های تحقیق و مقالات علمی در زمینه های امنیت سایبری
c. آشنایی با ابزار های مختلف تحلیل حملات سایبری (ویب، شبکه و موبایل)
d. بلدیت کامل با سیستم های عامل لینوکس و نرم افزار های کود باز
e. آشنایی با استندرد های امنیت سایبریISO IEC، SANS ، PCI-DSS ، COBIT,ISMS,CHFI,ISCSA