



میریت حفاظتی فن آوری های نوین

تألیف

ناصر کامیار

دانشگاه اطلاعات و امنیت ملی

مؤسسه چاپ و انتشارات

۱۳۹۷

سرشناسه	: کامیار، ناصر
عنوان و نام پدیدآور	: مدیریت حفاظتی فن‌آوری‌های نوین / تألیف ناصر کامیار
مشخصات نشر	: تهران: دانشگاه اطلاعات و امنیت ملی، موسسه چاپ و انتشارات، ۱۳۹۶.
مشخصات ظاهری	: ۳۹۵ ص. ش ۳۹۵
وضعیت فهرست‌نویسی	: فیا
موضوع	: تکنولوژی اطلاعات - تدابیر ایمنی
موضوع	: Information technology—Security measures
موضوع	: کامپیوترها - ایمنی اطلاعات
موضوع	: Computer security
موضوع	: منابع اطلاعاتی الکترونیکی - کنترل دستیابی - حفاظت داده‌ها
موضوع	: Electronic information resources—Access control—Data protection
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. معاونت پژوهش و تولید علم
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. موسسه چاپ و انتشارات
رده‌بندی کلاس	: ۱۳۹۶ م ۵/۵۸/۵ T
رده‌بندی دیوین	: ۳۰۳۰۸۳۳
شماره کتابشناسی	: ۵۰۶۵۹

مشخصات

عنوان: مدیریت حفاظتی فن‌آوری‌های نوین

تألیف: ناصر کامیار

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی

تاریخ انتشار: ۱۳۹۷

نوبت چاپ: اول

شمارگان: ۵۰۰ نسخه

بها: ۲۰۰,۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۸۸۸۵-۲۹-۰

«تمامی حقوق این اثر محفوظ است. تکثیر یا تولید مجدد آن کلی یا جزئی به هر صورت (چاپ،

فتوکی، صوت، تصویر و انتشار الکترونیکی) بدون اجازه مکتوب ناشر ممنوع است.»

تلفن: ۲۲۴۶۹۷۳۹

تهران: صندوق پستی ۱۴۳۸-۱۶۷۶۵

فهرست مطالب

مقدمه ناشر	۵
پیشگفتار	۱۷

فصل اول

آشنایی با کلیات علم مدیریت و امنیت اطلاعات

آشنایی با علم مدیریت	۲۴
آشنایی با فن آوری های نوین اطلاعاتی	۲۶
عناصر اصلی فن آوری اطلاعات	۲۷
زمینه های فن آوری اطلاعات	۲۸
حریم خصوصی و فن آوری اطلاعات	۲۹
نتیجه گیری	۵۳

فصل دوم

کارکردهای سیستم های اطلاعاتی در رابطه با فن آوری های نوین اطلاعاتی

کارکردهای سیستم های اطلاعاتی در رابطه با فن آوری های نوین اطلاعاتی	۵۸
وظایف حراست برای رسیدن به اهداف	۶۰
نقش حراست در پیشگیری از وقوع تخلف ها	۶۱
کارکردهای درون سیستمی و ملی	۶۲
اقدامات و نقش های مرتبط با تدوین سیاست نامه، آیین نامه و ابلاغ بخشنامه	۶۳
اقدامات و نقش های مرتبط با شبکه ها و کامپیوترهای داخلی سازمان	۶۴
اقدامات و نقش های مرتبط با اینترنت مورد استفاده در سازمان	۶۷
اقدامات و نقش های مرتبط با سیستم های مخابراتی سازمان	۶۸
اقدامات و نقش های مرتبط با توجیه و آموزش کارکنان و مدیران مرتبط با ابزار نوین	۷۱
اقدامات مرتبط با تعیین صلاحیت مربوط به فن آوری اطلاعات	۷۱

اقدامات و نقش‌های مرتبط با نظارت و بازرسی مربوط به استفاده از ابزار نوین فن‌آوری در سازمان.....	۷۲
نتیجه‌گیری.....	۷۳

فصل سوم

دولت سیار

دولت الکترونیک.....	۷۶
مفهوم حکمرانیت‌داری خوب.....	۷۸
ساختار دولت الکترونیک.....	۷۹
روند ایجاد دولت الکترونیک.....	۸۰
اهمیت ایجاد دولت الکترونیک.....	۸۱
مهم‌ترین عوامل ایجاد دولت الکترونیک.....	۸۲
مزایای دولت الکترونیک.....	۸۳
استراتژی استقرار دولت الکترونیک.....	۸۵
تعریف ساختار دولت الکترونیک و ابزار و عناصر کلیدی آن.....	۸۶
راهکارهای دولت الکترونیکی.....	۸۷
اهداف دولت الکترونیک.....	۸۸
تحقق دولت الکترونیکی.....	۹۱
مراحل پیاده‌سازی دولت الکترونیکی.....	۹۲
کانال‌های ارتباطی.....	۹۲
مشتریان دولت الکترونیک.....	۹۳
رسانه منتخب برای دولت الکترونیک.....	۹۴
تعیین مخاطبان و کاربران دولت الکترونیک.....	۹۴
موانع ایجاد دولت الکترونیک و چالش‌های آن.....	۹۴
نقش سازمانی عوامل حراستی در رابطه با فن‌آوری‌های نوین به‌کار گرفته شده در دولت سیار.....	۹۵
چالش‌های امنیتی دولت سیار.....	۹۵
نتیجه‌گیری.....	۱۰۳

فصل چهارم

اسناد غیر دیجیتال

۱۰۹	 سند (مدرک)
۱۱۰	 اسناد غیر دیجیتال و انواع آن
۱۱۴	 سند از دیدگاه بایگانی
۱۱۵	 تقسیم‌بندی سند
۱۱۵	 سند و انواع ارزش‌های آن
۱۱۶	 مدیریت بر اسناد غیر دیجیتال
۱۱۸	 پرونده
۱۲۲	 رابطه‌سازی بین اسناد غیر دیجیتال و فن‌آوری‌های نوین اطلاعاتی
۱۲۹	 ردیابی دیجیتال اسناد مهم
۱۲۹	 مدیریت حفاظتی بر فن‌آوری‌های نوین در اسناد غیر دیجیتال
۱۳۷	 نتیجه‌گیری

تصل جم

اطلاعات ذهنی

۱۴۰	 نقش ذهن و مغز در انباشت‌سازی اطلاعات
۱۴۷	 نظریه سیناپسی در فیزیولوژی یادگیری و حافظه
۱۴۸	 نظریه مبتنی بر الکتروفیزیولوژی و تشکیل مدارهای حافظه در فیزیولوژی یادگیری و حافظه
۱۴۹	 تفاوت حافظه کوتاه مدت و دراز مدت از لحاظ فیزیولوژی
۱۵۰	 تأثیر عوامل مختلف بر جریان فیزیولوژیکی یادگیری و حافظه
۱۵۱	 حقایق اعجاب‌انگیز درباره مغز انسان
۱۵۳	 مدیریت حفاظتی بر اطلاعات ذهن
۱۵۴	 تاریخچه حافظه
۱۵۵	 انواع حافظه
۱۶۱	 مراحل حافظه
۱۶۳	 سنجش حافظه

۱۶۴	فراموشی
۱۷۰	تمرکز حواس
۱۷۱	مدیریت حفاظتی بر فن آوری های نوین مرتبط با اطلاعات ذهنی
۱۷۵	نتیجه گیری

فصل ششم

تهدیدات فن آوری های نوین سازمانی در مراحل مختلف به کار گیری

۱۷۸	جنگ اطلاعاتی
۱۷۹	اختلافات، دزدان حقیقی و مجازی
۱۸۱	جهانی سازی
۱۸۲	مشخصه تهدیدات سایبری
۱۸۵	حملات داخلی مخرب
۱۸۷	اقدامات کاهش ریسک
۱۹۷	نتیجه گیری

فصل هفتم

رمز و رمزنگاری در ابزار نوین

۲۰۰	رمز و رمزنگاری در ابزار نوین
۲۰۰	تعاریف و مفاهیم رمزنگاری
۲۰۱	تاریخچه رمزنگاری
۲۰۴	اهداف رمزنگاری پیشرفته
۲۰۵	انواع حمله ها به رمز از نظر دشمن
۲۰۵	انواع شیوه های پایه رمزنگاری
۲۱۱	رمزنگاری مبدأ به مقصد و رمزنگاری انتقال
۲۱۳	الگوریتم های رمزنگاری متقارن
۲۲۱	الگوریتم های رمزنگاری با کلید نامتقارن
۲۲۵	پنهان سازی و پنهان نگاری در ابزار نوین
۲۳۱	مدیریت حفاظتی بر چرخه رمزنگاری و پنهان نگاری اطلاعات

۲۳۸	انواع حملات قابل اجرا بر روی الگوریتم
۲۳۹	چهار نوع عمومی از حمله‌های رمزنگاری
۲۴۱	ملزومات طرح مؤثر و کارای نرم‌افزاری الگوریتم رمز
۲۴۷	الگوریتم‌های تبادل کلید
۲۴۸	نتیجه‌گیری

فصل هشتم

مدیریت ریسک مرتبط با اطلاعات ابزار نوین

۲۵۲	ارزیابی ریسک
۲۵۵	ارزیابی مستمر شناسایی مداوم ریسک‌های مربوط به مأموریت فن‌آوری اطلاعات
۲۵۷	فهرست نمونه‌ای از انواع ریسک‌های قابل اعمال بر سازمان مبتنی بر فن‌آوری اطلاعات
۲۵۷	شرح ریسک‌های مرتبط با نرم‌نگی سرمایه‌های اطلاعاتی سازمان
۲۶۰	شرح ریسک‌های مرتبط با در دسترس بودن سرمایه‌های اطلاعاتی سازمان
۲۶۱	عوامل موفقیت در مدیریت ریسک فن‌آوری
۲۶۲	تصمیم‌گیری چیست؟
۲۶۳	سطوح تصمیم‌گیری
۲۶۴	درجه سختی تصمیم‌گیری
۲۶۵	انواع تصمیم‌گیری بر مبنای اطلاعات موجود
۲۶۸	فرآیندهای تصمیم‌گیری
۲۶۹	رویکردهای تصمیم‌گیری
۲۷۰	مدل‌سازی برای تصمیم
۲۷۱	تصمیم‌گیری به روش AHP
۲۸۱	مدیریت حفاظتی بر مدیریت ریسک و تصمیم‌گیری در رابطه با اطلاعات فن‌آوری‌های نوین
۲۸۳	انواع دارایی‌های یک سازمان
۲۸۳	نتیجه‌گیری

فصل نهم

مدل سازی امنیتی

سیاست های کنترل دسترسی	۲۸۸
انواع مدل های امنیت اطلاعات کامپیوتری	۲۸۸
کنترل دسترسی در نرم افزار	۲۹۴
انواع مدل های کنترل دسترسی	۲۹۵
قوانین بایه ای حاکم بر سیستم مبتنی بر نقش	۲۹۹
کنترل دسترسی مبتنی بر قوانین	۲۹۹
معرفی انواع کنترل های دسترسی	۳۰۰
نقش مدیریت حفاظتی در مدل سازی امنیتی و حراستی	۳۰۷
نتیجه گیری	۳۰۹

فصل دهم

قوانین حاکم بر فن آوری های نوین

نقش قوانین ساختاری و حاکمیتی در حفظ امنیت فن آوری اطلاعات مرتبط با فن آوری های نوین	۳۱۵
انواع قوانین مصوب در امر اطلاعات مرتبط با فن آوری های نوین	۳۱۶
قانون اساسی جمهوری اسلامی	۳۱۹
قانون رسیدگی به تخلفات اداری	۳۱۹
آیین نامه اجرائی قانون رسیدگی به تخلفات اداری	۳۲۰
قانون مجازات اسلامی	۳۲۲
آیین دادرسی کیفری	۳۲۵
قانون کارشناسان رسمی دادگستری مصوب ۱۳۸۱/۱/۱۸	۳۲۵
قانون مطبوعات مصوب ۶۴/۱۲/۲۸ و طرح اصلاحی مصوب ۱۳۷۹	۳۲۶
قانون مجازات و جرایم نیروهای مسلح	۳۲۷
آیین نامه طرز نگهداری اسناد سری و محرمانه دولتی مصوب ۱۳۵۴/۱۰/۱	۳۲۸
آیین نامه اجرایی اسناد طبقه بندی شده وزارت امور خارجه جمهوری اسلامی مصوب ۱۳۶۵/۴/۴	
	۳۳۳

۳۳۳	شرح قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی
۳۳۶	ماده ۵۰۱ قانون مجازات اسلامی
۳۵۱	ماده ۶۴ قانون تعزیرات سابق
۳۵۲	الزامات امنیتی افتا
۳۵۳	آیین نامه حفاظت از اسناد و مدارک
۳۶۵	نقش عملیاتی ساختارهای حفاظتی و حراستی مرتبط با قوانین
۳۶۷	نتیجه گیری

فصل یازدهم

آینده پژوهی در امر اطلاعات مرتبط با فن آوری های نوین

۳۷۳	تعریف آینده پژوهی
۳۷۴	اهمیت آینده پژوهی
۳۷۴	اهمیت آینده پژوهی از دیدگاه آینده پژوهان
۳۷۵	اهداف کلی آینده پژوهی
۳۷۵	مؤلفه های موفقیت آینده پژوهی؛ ابزاری برای ساخت آینده
۳۸۲	آینده پژوهی در امر اطلاعات مرتبط با فن آوری های نوین
	نقش قوانین ساختاری و حاکمیتی در حفظ و نگهداری اطلاعات و نقش عملیاتی و مدیریت های
۳۸۷	حفاظتی و حراستی در انطباق ساختاری با آینده پژوهی اطلاعات مرتبط با فن آوری های نوین
۳۸۸	نتیجه گیری
۳۹۱	منابع و مآخذ

پیشگفتار

با ظهور و رشد فن‌آوری‌های نوین، فضای سایبر یکی از ارکان اساسی اداره جوامع امروزی به‌شمار می‌رود. عرضه بخش بزرگی از خدمات عمومی و سهولت و سرعت انجام کار و امکانات گسترده فضای سایبری و فن‌آوری اطلاعات آن را به مهم‌ترین عرصه برای فعالیت سرمایه‌ای ملی تبدیل نموده است.

آمریکا شیطان بزرگ و ابدی و بزرگ‌ترین بازیگر فعال در فضای مجازی محسوب می‌شوند که با طراحی و سرمایه‌گذاری و تولید دانش و فن‌آوری‌های نوین بیش‌ترین بهره‌برداری از فضای مجازی را کسب نموده و فضای سایبر را به میدان برنامه‌ریزی راهبردی و هدایت مزیت‌های تاکتیکی در جهت دستیابی به اهداف سلطه طلبانه و به یکی از عرصه‌های تقابل میان کشورها و قدرت‌های دنیای تبدیل نموده است.

اسناد و مدارک طبقه‌بندی شده هر کشور جزء دارایی‌های ملی با ارزش آن محسوب شده و حفاظت از آنها بر مبنای دلایل عقلی و قانونی اجتناب‌ناپذیر بوده و یکی از وظایف واحدهای مسئول در این رابطه می‌باشد، زیرا افشای آنها منجر به استرسی افراد غیرمجاز به‌ویژه دشمنان، رقبای و کسانی که به هر دلیلی به دنبال سوءاستفاده از آن اسناد و اطلاعات می‌باشند ضربات جبران‌ناپذیری به اساس حکومت، منافع ملی، منافع کشور و یا یک سازمان وارد می‌کند.

از دیرباز تاکنون افشاء غیرمجاز اطلاعات و اسناد طبقه‌بندی شده مشکلات عدیده‌ای برای حکومت‌ها، دولت‌ها و سازمان‌ها ایجاد کرده و در برخی موارد موجب به‌روز جنگ‌ها و آشوب‌هایی شده و خسارت‌های سنگین جانی و مالی به ملت‌ها تحمیل نموده است. در کشورمان نیز نمونه‌های متعددی از جمله مواردی در طی دوران دفاع مقدس و پس از آن وجود دارد که تبعات جبران ناپذیری برای نظام داشته است.

فرآیند تولید، گردش و نگهداری اسناد طبقه‌بندی شده و بهره‌برداری بهینه از آن‌ها و انجام امور حفاظتی مربوطه و نظارت بر واحدهای زیر مجموعه مستلزم استقرار یک نظام صریح و اصولی در امر حفاظت از اسناد و اجرای دقیق آن از سوی مدیران و کارکنان می‌باشد. دستیابی و افشای غیرمجاز اسناد و مدارک طبقه‌بندی شده دلایل متعددی دارد که از مهمترین آن‌ها عدم شناخت و آگاهی نسبت به ارزش اطلاعات و اسناد طبقه‌بندی شده در اختیار، عدم اطلاع از تبعات افشاء آن‌ها، سهل انگاری، بی‌توجهی و بی‌دقتی در انجام وظایف محوله اداری و اصول حفاظتی است.

در رابطه با حفظ و نگهداری اطلاعات احادیث بسیاری از ائمه وارد شده است که آگاهی از آن وظیفه همه را در این رابطه سنگین‌تر می‌نماید.

الإمام الصادق عليه السلام: سرُّك مِن دَمِكَ فلا يَجْرِيَنَّ مِن عَمَلِكَ أَوْدَاجُكَ

راز تو جزئی از خون توست، پس نباید که در گهری غیر تو جریان یابد (بحار الانوار، ج ۷۲: ۷۱).

در سازمان‌های مختلف دولتی و عمومی مسئولیت حفظ و نگهداری اطلاعات تولید شده بنا بر ابلاغ صریح شورای عالی امنیت ملی با تولید کننده اطلاعات بوده و معمولاً مدیران سازمان‌ها این وظیفه را به قسمت‌های حراست سازمان خود تفویض اختیار می‌نمایند.

برای ایفای این نقش، افراد و مدیران شاغل در حراست و یا حفاظت مجموعه نیازمند آشنایی بیش‌تر با وظایف خود می‌باشند. در این کتاب وظایف مدیریتی و فنی مورد نیاز مدیران حراست فن‌آوری اطلاعات سازمان‌ها مورد بحث قرار می‌گیرد.

مخاطب اصلی این کتاب دانشجویان کارشناسی ارشد رشته حفاظت و مشابه آن در دانشگاه اطلاعات و امنیت ملی می‌باشد و به صورت عمومی کلیه افرادی که در قسمت‌های حراستی و یا حفاظتی به عنوان مدیر و یا کارشناس مشغول به خدمت بوده و یا علاقه‌مند به خدمت در این‌گونه مشاغل می‌باشند می‌توانند از مطالب کتاب در راستای مدیریت به خود استفاده نمایند.

این کتاب در ۱۱ فصل تقدیم خوانندگان شده و در هر فصل ضمن برشمردن نکاتی در مورد یکی از وظایف مدیریتی در راستای حفاظت از فن‌آوری‌های نوین، دارای سؤالاتی در انتهای فصل می‌باشد که خوانندگان با توانایی بر پاسخ آن می‌توانند دانسته‌های خود را مورد آزمون قرار دهند. اساتید محترم نیز پس از بهره‌برداری از این کتاب به عنوان منبع اصلی درس مدیریت حفاظتی به فن‌آوری‌های نوین می‌توانند از سؤالات انتهای هر فصل به عنوان آزمون‌های پایانی، ترم بهره بگیرند.

اساتید محترم در اثنای تدریس هر فصل از مصادیق موجود در سازمان‌های هم‌عرضی که دانشجویان در آن‌جا مشغول به کار می‌باشند بهره‌گیری فرمایند تا یادگیری دانشجویان عینی‌تر باشد.

در فصل اول کتاب اصول کلی مرتبط با فن‌آوری‌های اطلاعات و مبحث حفاظت برای یادآوری دانشجویان به صورت کلی بیان شده است تا مخاطبان با تعاریف عملیاتی که در طول کتاب درباره حفاظت و مدیریت و فن‌آوری‌های نوین قید می‌گردد دارای مفاهیم یکسانی باشند.

وظیفه سیستم‌های اطلاعاتی در قانون و بخشنامه‌های صادره بالادستی در کشور به صورت شفاف بیان شده است. برخی از این وظایف در سطح کلان کشور و منطقه بوده و برخی از آن‌ها کاربرد ملی و درون سازمانی دارند. به این گونه مباحث در فصل دوم پرداخته شده است تا دانشجویان با این نقش‌ها آشنا شده و بر آن مبنای بتوانند مطالب را فرا گیرند.

در فصل سوم به بحث دولت الکترونیک و در همان راستا عبور از دولت الکترونیک و تبدیل شدن آن به دولت سیار پرداخته شده است. امروزه با رشد فن‌آوری‌های نوین اطلاعات و ارتباطی، کشورها الزاماً می‌بایست به این عرصه وارد شوند تا بتوانند نیازهای مردمان کشور خود را در کوتاه‌ترین زمان و به بهترین شکل و با دقت و سرعت لازم برآورده نمایند. این کار به غیر از ورود در عرصه دولت سیار امکان‌پذیر نمی‌باشد. در این فصل دانشجویان با ویژگی‌های عمومی و حفاظتی دولت سیار آشنا شده و نقش نیروهای حراستی در این قانون اعمال حاکمیت را فرا می‌گیرند و با وظایف صیانتی خود در دولت سیار آشنا می‌شوند.

سازمان‌ها در حال گذر از اطلاعات سنتی به سمت اطلاعات دیجیتال می‌باشند و در این گذر الزاماً تا سالیان سال نمی‌توان نقش اسناد غیر دیجیتال در سازمان‌ها را نادیده گرفت. در این دوره گذر بعضاً از ابزار نوین برای مدیریت بر اسناد غیر دیجیتال در سازمان‌ها استفاده می‌شود. در فصل چهارم این مسئله مورد بحث و بررسی قرار می‌گیرد تا دانشجویان ضمن آشنایی با ویژگی‌های این دوره گام بردارند بهترین مشورت‌های صیانتی را به مدیران سازمان ارائه نمایند.

فصل پنجم به اطلاعات رسوب شده در حافظه می‌پردازد. ذهن از جمله ابزار ذخیره‌سازی است که به هیچ شکل دیگری غیر از خود کتلی شاید نتوان بر آن مدیریت نمود. در این فصل وضعیت و شیوه‌های رسوب اطلاعات در ذهن و نوع به

یادآوری و ارائه آن به بیرون از ذهن و شیوه‌های کمک به خود مدیریتی افراد مورد بحث و بررسی قرار می‌گیرد. اطلاعات در چرخه‌ای کامل در سازمان‌ها تولید، پردازش، نگهداری و توزیع می‌شود. قبل از تولید نیز فرآیندهای خاص مدیریتی و حراستی در سازمان‌ها انجام می‌شود تا آسیب‌پذیری تولید و ادامه فرآیند را ایمن‌تر نماید.

در فصل ششم به این مهم پرداخته شده و در هر قسمت از آن وظایف صیانتی که می‌بایست توسط کارمندان حراست که همان دانشجویان فعلی می‌باشد یا باید به‌کار بسته شوند و بر اساس آن استنتاج برای شیوه برخورد با مسئله به دست آید عنوان شده است. با توجه به اینکه یکی از روش‌هایی که دشمنان می‌توانند به اطلاعات دسترسی یابند در مرحله توزیع می‌باشد و اگر اطلاعات با شیوه صحیحی رمزنگاری شده باشند دشمن یا توان دسترسی به اطلاعات را نخواهد داشت و یا این‌که هزینه و زمان بسیار زیادی را باید صرف نماید.

در فصل هفتم به مسئله انواع رمز و رمزنگاری و نکاتی که می‌بایست توسط نیروهای حراستی مدنظر قرار گیرد پرداخته شده است. با توجه به این‌که امروزه علاوه بر رمزنگاری از شیوه‌های پنهان‌سازی اطلاعات نیز بهره گرفته می‌شود در این فصل تلاش شده است به بحث استگنوگرافی که همان پوشش دادن به اطلاعات می‌باشد نیز پرداخته شود تا دانشجویان بتوانند با شیوه‌های حراست از این روش‌ها آشنا گردند. در دوره سیستمی هر اقدامی که بخواهد انجام شود معمولاً باید از یک مدل استاندارد تبعیت نماید و امروزه برای اعمال دسترسی به اطلاعات در شیوه‌های مختلف برنامه‌نویسی از مدل‌هایی استفاده می‌نمایند که در بسیاری از مناطق دنیا به صورت استاندارد درآمده است. در فصل نهم دانشجویان با انواع مدل‌های رایج مورد استفاده در کنترل دسترسی آشنا شده و توان خود را در نظارت مربوطه در سازمان‌ها افزایش می‌دهند.

فصل دهم به قوانین موضوعه در امر فن‌آوری اطلاعات در کشور پرداخته و انواع قوانینی که برای ایفای نقش حفاظتی و حراستی دانشجویان به آن نیاز دارند مورد بحث و بررسی قرار گرفته است. در این فصل تلاش شده است که وارد مباحث فنی حقوقی شویم ولی به میزانی که دانشجویان برای ایفای نقش صیانتی خود به آن نیاز دارند پرداخته شده است.

در انتهای کتاب در فصل یازدهم بحث آینده پژوهی و نگاه به آینده فن‌آوری نوین و نقش حیاتی آن پرداخته شده است و دانشجویان با گذراندن این فصل توان آن را پیدا خواهند کرد تا با نگاه آینده پژوهانه به استقبال خطراتی که در آینده در بعد مدیریت حفاظت، بر فن‌آوری‌های نوین روبرو خواهند شد پرداخته می‌شود.

در انتهای هر فصل از کتاب سؤالاتی که در برگیرنده کل فصل بوده و با ارزش آزمون دو نمره از بیست نمره است. اساتید محترم می‌توانند برای آزمون پایان کلاس از سؤالات فوق بهره‌مندی نمایند.

با امید موفقیت تمامی سربازان و حافظان نظام مقدس جمهوری اسلامی ایران.

ناصر کامیار

مستان ۹۶