۹۵/۳/۱۹

ISO/IEC 27001&27002 (2013)

بخش اول: استاندارد ISO/IEC 27001:2013

بخش دوم: استاندارد ISO/IEC 27002:2013

بخش سوم: تغییرات ویرایش 2013 نسبت به ویرایش 2005

مترجم و مولف : رضا طی

موسس و مدیر عامل

شرکت مهندسی کاربرد سیستم سدید

(کاسیس)

سرشناسه	: طی‌نیا، رضا، ۱۳۵۵ -
عنوان و نام پدید آور	: استاندارد (ISO/IEC ۲۷۰۰۱&۲۷۰۰۲:۲۰۱۳)/ترجمه و تالیف رضا طی‌نیا.
مشخصات نشر	: تهران: فن‌آوران، ۱۳۹۵.
مشخصات ظاهری	: ۴۰۲ ص.: مصور
شابک	: ۹۷۸-۶۰۰-۳۱۹-۰۹۰-۰
وضعیت فهرست نویسی	: فیپا
موضوع	: تکنولوژی اطلاعات -- تدابیر ایمنی -- استانداردها
موضوع	: شبکه‌های کامپیوتری-- تدابیر ایمنی--استانداردها.
موضوع	: کامپیوترها -- ایمنی اطلاعات -- استانداردها.
موضوع	: حفاظت داده‌ها -- استانداردها.
رده بندی کنگره	: ۱۳۹۵ ۵الف۹۴ط/T۵۸/۵
رده بندی دیویی	: ۳۰۳/۴۸۳۳
شماره کتابشناسی ملی	: ۴۱۸۲۶۵۱

نشر فن آوران

ISO/IEC 27001&27002 (2013)

- **تالیف و ترجمه : رضا طی نیا**
- نوبت چاپ: اول: ۱۳۹۵
- چاپ و صحافی: مرتب
- شمارگان: ۱۰۰۰ نسخه
- شابک: ۹۷۸-۶۰۰-۳۱۹-۰۹۰-۰ **قیمت: ۴۵۰۰ تومان**

نشانی پخش: تهران، خیابان انقلاب، خیابان بهار جنوبی، برج بهار، طبقه د[illegible]ری، واحد ۷۳۸

تلفن : ۸۸۵۴۵۱۲۴ - ۷۷۶۴۲۹۶۶

کاسیس

شرکت مهندسی کاربرد سیستم سدید (کاسیس) در سال ۱۳۸۷ تأسیس گردیده و فعالیت خود را در حوزه های مختلف ارائه خدمات صدور گواهینامه، آموزش، و ممیزی در بخش های مختلف سیستم های مدیریت کیفیت و مدیریت فناوری اطلاعات آغاز نمود، با توجه به نیاز روزافزون مشتریان به خدمات مختلف در سطوح استراتژیک، **(کاسیس)** فعالیت‌های مرتبط با مشاوره در حوزه‌های مختلف را به عنوان بخش تکمیلی فعالیت‌هایخود برگزید و برای تکمیل سبد ارائه خدمات به مشتریان و در راستای ایجاد اطمینان خاطر، ارائه تجهیزات و نرم افزارهای مرتبط و سیستم‌های یکپارچه مالی و اداری را نیز به مجموعه خدمات خود افزوده است که این خدمات توسط شرکت یا شرکای تجاری داخلی و خارجی و به صورت بسته‌های کامل و یکپارچه به مشتریان عرضه می‌گردد.

بر اساس خط مشی کاری شرکت، شرط پایداری ارتباط با مشتریان و کلید اصلی توسعه شرکت جلب رضایت مشتری و تداوم این رضایتمندی می باشد. در همین راستا **شرکت مهندسی کاربرد سیستم سدید (کاسیس)** تلاش می کند با بررسی جداگانه روند کاری هر یک از مشتریان نسبت به ارائه مشاوره جهت رفع نیازها و کارکرد بهینه پرسنل شرکت های طرف قرارداد اقدام نماید. بخش های تولید مشاوره، آموزش و ممیزی، **(کاسیس)**، وظیفه ارتباط و تامین نیازها و [illegible] قشر وسیع از خانواده کاربرد سیستم را بر عهده دارند که با قرار دادن [illegible] روش موازی در دستور کار سعی در برطرف نمودن نیاز و جلب رضایت مشتریان را می نماید.

شرکت مهندسی کاربرد سیستم سدید (کاسیس)، در سال ۱۳۹۲، موفق به اخذ نمایندگی از موسسه آزمایشی و صدور گواهینامه PECB (کانادا) گردید، این موسسه در حوزه آموزش و صدور گواهینامه انطباق سیستم‌های مدیریت امنیت، کیفیت، زیست محیط، انرژی و ... فعالیت می‌کند و یکی از معدود موسساتی در دنیا می‌باشد که تائید موسسات معتبری مثل موسسه ملی استاندارد آمریکا (IAS-IAF) را دارد

شرکت مهندسی کاربرد سیستم سدید (کاسیس)، در سال ۱۳۹۴، موفق به اخذ نمایندگی از موسسه آموزشی I'Pre...urs (فرانسه) گردیده، و به عنوان اولین شرکت دارای نمایندگی رسمی از این شرکت در ایران به ارائه خدمات به مشتریان می پردازد

این شرکت همچنین در سال ۱۳۹۱ موفق به اخذ مجوز از سازمان فناوری اطلاعات ایران **(نما)** در حوزه‌های مشاوره و آموزش سیستم مدیریت امنیت اطلاعات ISMS شده است

این شرکت در سال ۱۳۹۱ موفق به اخذ گواهینامه های ISO27001 , ISO9001 گردیده است

این شرکت مشتری را شریک تجاری خود دانسته و هدف خود را رسیدن به رضایت بالای مشتری می داند.

فهرست

پیشگفتار

ISO (سازمان بین‌المللی استاندارد) و IEC (کمیسیون بین‌المللی الکتروتکنیک) باهم سازمان تخصصی برای استانداردسازی جهانی را تشکیل می‌دهند. آن گروه از مؤسسات ملی که از اعضای ISO یا IEC محسوب می‌شوند، از طریق کمیته‌های فنی که توسط سازمان‌های مربوطه تشکیل‌شده‌اند، در تدوین استانداردهای جهانی همکاری می‌نمایند و حوزه‌های خاص فعالیت‌های فنی را مورد بررسی قرار می‌دهند. هم‌چنین کمیته‌های فنی و تخصصی سازمان‌های ISO و IEC در موضوعاتی که موردعلاقه طرفین باشد به همکاری مشترک اقدام می‌کنند. سایر سازمان‌های بین‌المللی دولتی و غیردولتی در کنار ISO و IEC در این کار همکاری می‌کنند. درزمینه‌ی کاری فناوری اطلاعات، ISO و IEC، کمیته فنی مشترکی را تشکیل داده‌اند که در اصطلاح ISO/IEC JTC 1 شناخته می‌شود.

پیش‌نویس استانداردهای بین‌المللی بر اساس مقررات و دستورالعمل‌های ISO/IEC تهیه می‌شوند.

وظیفه اصلی کمیته فنی مشترک، تهیه استانداردهای جهانی به شمار می‌آید. نسخه پیش‌نویس استانداردهای جهانی که توسط کمیته فنی مشترک پذیرفته‌شده‌اند برای رأی‌گیری به مجامع ملی ارسال می‌شوند. انتشار استاندارد به‌صورت بین‌المللی نیازمند تائید توسط حداقل ۷۵ درصد از آرا مجامع و سازمان‌های ملی است.

توجه به این نکته قابل‌توجه است که ممکن است بعضی از بخش‌های این مستند مشمول حقوق ثبت اختراعات شوند. در این خصوص ISO و IEC مسئولیتی در قبال تمام یا بخشی از این حقوق بر عهده نخواهند داشت.

ISO/IEC 27001 توسط کمیته مشترک فنی ISO/IEC JTC 1، فناوری اطلاعات، کمیته فرعی SC 27 و تکنیک‌های امنیتی فناوری اطلاعات تدوین‌شده است.

این نسخه، به‌عنوان نسخه دوم، ویرایش اول (ISO/IEC 27001:2005) را لغو کرده و بر اساس بازبینی فنی صورت گرفته، جایگزین آن می‌گردد.

۰ مقدمه

۰-۱ کلیات

هدف از تدوین این استاندارد بین المللی، تعیین الزامات جهت استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات است. پذیرش سیستم مدیریت امنیت اطلاعات، تصمیمی راهبردی برای سازمان است. استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات تحت تأثیر نیازها و اهداف و الزامات امنیتی سازمان، فرایندهای سازمانی مورداستفاده و اندازه و ساختار سازمان است. انتظار می‌رود به‌مرور زمان، همه این عوامل تأثیرگذار، تغییر کند. سیستم مدیریت امنیت اطلاعات از محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات با به‌کاربردن فرایند مدیریت مخاطرات محافظت می‌کند و به علاقه‌مندان اطمینان می‌دهد که مخاطرات به حد کافی مدیریت می‌شود.

... است که سیستم مدیریت امنیت اطلاعات، جزئی از فرایندهای سازمان و ساختار کلی مدیریتی و به‌صورت یکپارچه با آن باشد و امنیت اطلاعات در ... فرایندها، سامانه‌های اطلاعاتی و کنترل‌ها در نظر گرفته شود. انتظار می‌رود پیاده‌سازی سیستم مدیریت امنیت اطلاعات، متناسب با نیازهای سازمان باشد.

این استاندارد بین المل... می‌تواند توسط طرف‌های درونی و بیرونی، برای ارزیابی توانایی سازمان در برآورد سازی الزامات امنیت اطلاعات خود سازمان به‌کاربرده شود.

سامانه مدیریت امنیت اطلاعات (ISMS) محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را از طریق پیاده‌سازی فرایندهای مدیریت مخاطره حفظ می‌نماید و این اطمینان را به علاقه‌مندان می‌دهد که مخاطرات به میزان مناسبی مدیریت شده‌اند.

توجه به این نکته مهم است که سامانه مدیریت امنیت اطلاعات (ISMS) به‌صورت بخشی و نیز یکپارچه در ارتباط با فرآیندهای سازمانی و ساختارهای مدیریتی پیاده‌سازی می‌شود و این‌که امنیت اطلاعات در طراحی فرآیندها، سامانه‌های اطلاعاتی و کنترل‌ها مورد توجه قرارگرفته است. انتظار می‌رود که پیاده‌سازی سامانه مدیریت امنیت اطلاعات (ISMS) با نیازهای سازمان متناسب شود.

این استاندارد بین‌المللی می‌تواند برای ارزیابی توان سازمان‌ها در کسب الزامات امنیت اطلاعات توسط بخش‌های داخلی و خارجی مورداستفاده قرار گیرد.