INSO-ISO-IEC

27018

1st.Edition
2016

Identical with

ISO/IEC 27018:2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران-ایزو-آی ای سی

۲۷۰۱۸

چاپ اول

۱۳۹۵

فناوری اطلاعات- فنون امنیتی – آیین کار برای حفاظت از اطلاعات قابل‌شناسایی شخصی (PII) در ابرهای عمومی که به‌عنوان پردازشگرهای PII عمل می‌کنند

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ICS: 35.040

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات - فنون امنیتی – آیین کار برای حفاظت از اطلاعات قابل‌شناسایی شخصی (PII) در ابرهای عمومی که به‌عنوان پردازشگرهای PII عمل می‌کنند»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون اداره کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
دوست‌محمدی، وحید (کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

اعضاء: (اسامی به ترتیب حروف الفبا)	**سمت و/ یا محل اشتغال:**
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
مغانی،مهدی (فوق لیسانس ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
ویراستار:	
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	مشاور رئیس مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی– آیین کار برای حفاظت از اطلاعات قابل‌شناسایی شخصی (PII) در ابرهای عمومی که به‌عنوان پردازشگرهای PII عمل می‌کنند» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و سی و ششمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۰۷/۰۶ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27018:2014, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

۰ مقدمه

۰-۱ پس‌زمینه و زمینه[1]

ارائه‌کنندگان خدمات ابری که تحت قرارداد با مشتریان خود، اطلاعات قابل‌شناسایی شخصی (PII) [2]را پردازش می‌کنند باید خدمات خود را به شیوه‌ای انجام دهند که به هر دو طرف اجازه برآورده کردن الزامات قوانین کاربست‌پذیر و مقررات پوشش حفاظت از PII را بدهد. الزامات و روشی که در آن، الزامات بین ارائه-کننده خدمات ابری و مشتریان، تقسیم می‌شود با توجه به حوزه قضایی، و با توجه به شرایط قرارداد بین ارائه‌کننده خدمات ابری و مشتری، متفاوت است. قوانینی که تعیین می‌کند چگونه PII مجاز به پردازش اطلاعات (یعنی جمع‌آوری، استفاده، انتقال و امحا) است گاهی اوقات به عنوان قانون حفاظت از داده‌ها ذکر می‌شود؛ PII گاهی اوقات به عنوان داده‌های شخصی و یا اطلاعات شخصی نیز نامیده می‌شود. تعهدات یک پردازشگر PII در حوزه‌های قضایی متفاوت است، که آن را به چالشی برای کسب‌وکارهای ارائه‌کننده خدمات رایانش ابری و در فضای چند ملیتی، تبدیل می‌کند.

ارائه‌کننده خدمات ابر عمومی هنگامی «پردازشگر PII» است که PII را با توجه به دستورالعمل‌های مشتری خدمات ابری، پردازش می‌کند. مشتری خدمات ابری، که رابطه قراردادی با پردازشگر PII ابر عمومی دارد، می‌تواند از یک فرد معمولی، یک «مالک PII»، که PII خود را در حالت ابری پردازش می‌کند، تا سازمان، «واپایش‌گر(کنترل‌کننده) PII»، که PII مربوط به بسیاری از مالکان PII را پردازش می‌کند، شامل شود. مشتری خدمات ابری ممکن است یک یا چند کاربر خدمت ابری مرتبط با آن در اختیار داشته باشد که استفاده از خدمات برای آن، تحت قرارداد با پردازشگر PII ابر عمومی امکان‌پذیر باشد. توجه داشته باشید که مشتری خدمات ابری، توانایی پردازش و استفاده از داده‌ها را دارد. مشتری خدمات ابری که واپایش‌گر PII نیز هست، ممکن است در معرض مجموعه‌ای گسترده‌تر از تعهدات مربوط به حفاظت از PII نسبت به پردازشگر PII ابر عمومی باشد. تمایز قائل شدن بین واپایش‌گر PII و پردازشگر PII ، متکی بر این است که پردازشگر PII ابر عمومی، اهداف پردازشیِ داده‌ای به غیر از آن‌هایی که توسط مشتری خدمات ابری تنظیم شده تا PII آن‌ها را پردازش کند و نیز عملیات لازم برای رسیدن به اهداف مشتری خدمات ابری، ندارد.

یادآوری- آنجا که پردازشگر PII ابر عمومی، داده‌های حساب مشتری خدمات پردازش ابری را پردازش می‌کند، ممکن است به عنوان واپایش‌گر PII برای این منظور عمل کند. این استاندارد چنین فعالیت‌هایی را پوشش نمی‌دهد.

مقصود از این استاندارد، هنگام استفاده به همراه اهداف و واپایش‌های امنیت اطلاعات در استاندارد ISO / IEC 27002، ایجاد مجموعه مشترک از دسته‌ها و واپایش‌های امنیتی است که می‌تواند توسط ارائه-کننده خدمات ابر عمومی پیاده‌سازی شده که به عنوان پردازشگر PII عمل کند. این موضوع دارای اهداف زیر است:

- کمک به ارائه‌کننده خدمات ابر عمومی برای انطباق با تعهدات کاربست‌پذیر هنگامی که به عنوان پردازشگر

1 - Background and context
2 - Personally identifiable information

PII، خواه چنین تعهداتی به طور مستقیم بر پردازشگر PII اعمال شود یا از طریق قرارداد.

- توانمند کردن پردازشگر PII ابر عمومی تا در مسائل مربوط شفاف باشد طوری که مشتریان خدمات ابری بتوانند خدمات مناسب مبتنی بر پردازش ابری PII را انتخاب کنند.

- کمک به مشتری خدمات ابری و پردازشگر PII ابر عمومی برای ورود به توافق قراردادی.

- فراهم کردن سازوکار برای اعمال ممیزی و حقوق و مسئولیت‌های ناشی از انطباق مشتریان خدمات ابری در مواردی که ممیزی هر یک از داده‌های مشتریان خدمات ابری میزبانی شده در محیط (ابری) سرور مجازی و چند قسمتی ممکن است به لحاظ فنی غیر عملی بوده و مخاطرات واپایش‌های امنیت شبکه‌های فیزیکی و منطقی را افزایش دهد.

این استاندارد جایگزین قوانین[1] و مقررات کاربست‌پذیر نیست، اما می‌تواند به تامین چارچوب قابل‌قبول مشترک برای ارائه‌کنندگان خدمات ابر عمومی، به‌ویژه آن‌هایی که در بازار چند ملیتی عمل می‌کنند، کمک کند.

۰-۲ واپایش‌های حفاظت PII برای خدمات رایانش ابر عمومی

این استاندارد برای سازمان‌ها و برای استفاده به عنوان مرجع جهت انتخاب واپایش‌های حفاظت PII در روند پیاده‌سازی سامانه مدیریت امنیت اطلاعات رایانش ابری بر اساس استاندارد ISO / IEC 27001 طراحی شده است، و یا به عنوان سند راهنما برای پیاده‌سازی واپایش‌های حفاظت PII است که معمولا برای سازمان‌های اقدام کننده به عنوان پردازشگر PII ابر عمومی پذیرفته شده است. به طور خاص، این استاندارد بر اساس استاندارد ISO / IEC 27002 تدوین شده و شرایط مخاطره خاص ناشی از آن دسته از الزامات محافظتی PII اعمال شده به ارائه‌کنندگان خدمات ابر عمومی پردازشگر و اقدام‌کننده به عنوان پردازشگر PII را در نظر می‌گیرد.

به طور معمول سازمان اجراکنندهٔ استاندارد ISO / IEC 27001 از دارایی اطلاعات خود حفاظت می‌کند. با این حال، در زمینه الزامات حفاظت PII برای ارائه‌دهنده خدمات ابر عمومی اقدام‌کننده به عنوان پردازشگر PII، سازمان از دارایی‌های اطلاعاتی که توسط مشتریانش به آن واگذار شده است، حفاظت می‌کند. پیاده‌سازی واپایش‌های استاندارد ISO / IEC 27002 توسط پردازشگر PII ابر عمومی، برای این منظور هم مناسب و هم ضروری است. این استاندارد موجب تقویت واپایش‌های استاندارد ISO / IEC 27002 می‌شود تا ماهیت توزیع شده مخاطره و وجود رابطه قراردادی بین مشتری خدمات ابری و پردازشگر PII ابر عمومی را تطبیق دهد. این استاندارد استاندارد ISO / IEC 27002 را به دو روش غنی می‌کند:

- راهنمای پیاده‌سازی کاربست‌پذیر برای حفاظت PII ابر عمومی، برای برخی از مجموعه واپایش‌های استاندارد ISO/IEC 27002 و

1 - Legislation

- پیوست الف مجموعه‌ای از واپایش‌های افزوده و راهنمای مرتبط در نظر گرفته شده برای پرداختن به الزامات حفاظت PII ابر عمومی که توسط مجموعه واپایش‌های ISO/IEC 27002 موجود پرداخته نشده را تامین می‌کند.

بسیاری از واپایش‌ها و راهنماها در این استاندارد به واپایش‌کننده PII نیز اعمال می‌شود. با این حال، واپایش‌کننده PII، در اکثر موارد، در معرض تعهدات افزوده که در اینجا مشخص نشده‌اند، خواهد بود.

۰-۳ الزامات حفاظت PII

مهم است که سازمان الزامات خود را برای حفاظت از PII شناسایی کند. سه منبع اصلی الزامات، به شرح زیر وجود دارند:

الف- الزامات قانونی، مقرراتی، تنظیمی و قراردادی: یک منبع تعهدات و الزامات قانونی، مقرراتی، تنظیمی و قراردادی است که باید سازمان، شرکای تجاری، پیمانکاران و ارائه‌کنندگان خدمات آن راضی باشند، و مسئولیت‌های اجتماعی و فرهنگی و محیط عملکرد آن‌ها را برآورده شود. ذکر این نکته توصیه می‌شود که تعهدات قانونی، مقرراتی و قراردادی ایجاد شده توسط پردازشگر PII ممکن است اجرای واپایش‌های خاصی را الزام‌آور کند و همچنین ممکن است مستلزم معیارهای خاص برای پیاده‌سازی آن واپایش‌ها باشد. این الزامات می‌توانند از یک حوزه قضایی به حوزه‌ی دیگر متفاوت باشند.

ب- مخاطره‌ها: منبع دیگر، از ارزیابی مخاطره‌های سازمان مرتبط با PII و در نظر گرفتن راهبرد و اهداف کلی کسب‌وکار سازمان ناشی می‌شود. از طریق ارزیابی مخاطره، تهدیدها شناسایی‌شده، آسیب‌پذیری و احتمال وقوع آن ارزیابی شده و تاثیر بالقوه آن برآورد می‌شود. استاندارد ISO / IEC 27005 راهنمای مدیریت مخاطره امنیت اطلاعات، شامل مشاوره در ارزیابی مخاطره، پذیرش مخاطره، تبادل اطلاعات مخاطره‌ای، پایش مخاطره و بازنگری مخاطره را تامین می‌کند. استاندارد ISO / IEC 29134 راهنمای ارزیابی تاثیر حریم خصوصی را فراهم می‌کند.

پ- خط‌مشی‌های شرکت: در حالی که بسیاری از جنبه‌های تحت پوشش خط‌مشی شرکت از تعهدات قانونی و اجتماعی و فرهنگی به دست می‌آیند، ولی همچنین ممکن است سازمان به طور داوطلبانه انتخاب کند که فراتر از معیارهای مشتق شده از الزامات بند الف را در نظر بگیرد.

۰-۴ انتخاب و پیاده‌سازی واپایش‌ها در محیط رایانش ابری

واپایش‌ها می‌توانند از این استاندارد انتخاب شوند (که شامل ارجاع واپایش‌ها از استاندارد ISO / IEC 27002، ایجاد مجموعه واپایش مرجع ادغامی برای بخش و یا کاربرد تعریف شده توسط دامنه می‌شود). در صورت نیاز، همچنین واپایش‌ها می‌توانند از مجموعه واپایش‌های دیگری انتخاب شوند، و یا واپایش‌های جدید می‌توانند برای نیازهای خاص، هر طور که مناسب است، طراحی شوند.

یادآوری- خدمات پردازش PII تامین شده توسط پردازشگر PII ابر عمومی می‌تواند به عنوان کاربرد رایانش ابری، و نه به عنوان بخشی در خودش، در نظر گرفته شود. با این وجود، در این استاندارد اصطلاح «بخش خاص» استفاده می‌شود، همان‌طور که اصطلاح متعارف مورد استفاده در استانداردهای دیگر در مجموعه استاندارد ISO/IEC 27000 است.

انتخاب واپایش‌ها وابسته به تصمیمات سازمانی بر اساس معیارهای پذیرش مخاطره، گزینه‌های برخورد با مخاطره، و مشی کلی مدیریت مخاطره اعمال شده به سازمان و از طریق موافقت‌نامه‌های قراردادی، مشتریان و تامین‌کنندگان آن بوده، و در معرض همه قوانین و مقررات ملی و بین‌المللی مربوطه قرار خواهد گرفت. جایی که در آن، واپایش‌ها از این استاندارد انتخاب نشود، نیاز است منطق حذف آن‌ها مستند شود.

علاوه بر این، انتخاب و پیاده‌سازی واپایش‌ها، وابسته به نقش واقعی ارائه‌کننده ابر عمومی در زمینه معماری مرجع رایانش ابری است (به استاندارد ISO / IEC 17789 مراجعه شود). بسیاری از سازمان‌های مختلف می‌توانند درگیر تامین خدمات زیرساختی[1] و کاربردی در محیط رایانش ابری شوند. در برخی شرایط، واپایش‌های انتخاب‌شده می‌توانند برای ردهٔ خاص خدمت در معماری مرجع رایانش ابری منحصربه‌فرد باشند. در موارد دیگر، نقش‌های مشترک در پیاده‌سازی واپایش‌های امنیتی می‌تواند وجود داشته باشد. توافقات قراردادی باید به طور واضح مسئولیت‌های حفاظت از PII همه سازمان‌های درگیر در ارائه یا استفاده از خدمات ابری، از جمله پردازشگر PII ابر عمومی، پیمانکاران آن و مشتری خدمات ابری تعیین کند.

واپایش‌ها در این استاندارد می‌تواند به عنوان اصول راهنما در نظر گرفته شده و برای اکثر سازمان‌ها کاربست‌پذیر باشند. این واپایش‌ها با جزئیات بیشتری همراه با راهنمای پیاده‌سازی در زیر توضیح داده شده است. اگر الزامات حفاظت از PII در طراحی سیستم اطلاعات پردازشگر PII ابر عمومی در نظر گرفته شود، پیاده‌سازی آن می‌تواند ساده‌تر باشد. چنین ملاحظاتی، عناصر مفهومی هستند که اغلب «طراحی دربردارنده‌ی حریم خصوصی» نامیده می‌شود. فهرست کتاب‌شناسی، اسناد مربوطه مانند استاندارد ISO / IEC 29101 را فهرست می‌کند.

۵-۰ تدوین راهنماهای افزوده

این استاندارد می‌تواند به عنوان نقطه شروعی برای تدوین دستورالعمل‌های حفاظت PII در نظر گرفته شود. امکان اینکه همه واپایش‌ها و راهنماها در این آیین‌کار کاربست‌پذیر نباشد، وجود دارد. علاوه بر این، ممکن است واپایش‌ها و راهنماهای افزوده‌ای که در این استاندارد آورده نشده است، مورد نیاز باشد. زمانی که اسناد حاوی واپایش‌ها یا راهنماهای افزوده تدوین شوند، ممکن است در این استاندارد ارجاعات متقابل به بندهایی که برای تسهیل وارسی کردن انطباقی توسط ممیزان و شرکای کسب‌وکار در جاهایی که کاربست‌پذیر باشد، مفید باشد.

۶-۰ ملاحظات چرخه عمر

PII چرخه عمر طبیعی دارد که عبارت است از خلق و ایجاد از ذخیره‌سازی، پردازش، استفاده و انتقال تا

1 - Infrastructure

تخریب تدریجی یا فروپاشی آن. مخاطرات PII می‌توانند در طول زندگی آن متفاوت باشند اما حفاظت از PII در تمام مراحل، تا حدی مهم باقی می‌ماند.

الزامات حفاظت از PII باید همان‌طور که هستند در نظر گرفته شود و سامانه‌های اطلاعات جدید از طریق چرخه عمرشان اداره می‌شوند.

فناوری اطلاعات- فنون امنیتی – آیین کار برای حفاظت از اطلاعات قابل‌شناسایی شخصی (PII) در ابرهای عمومی که به‌عنوان پردازشگرهای PII عمل می‌کنند

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین اهداف واپایشی، واپایش‌ها و راهنماهای پذیرفته شده به‌طور مشترک برای پیاده‌سازی اقدامات برای محافظت از اطلاعات قابل‌شناسایی شخصی (PII) مطابق با اصول حریم خصوصی در استاندارد ISO/IEC 29100 در محیط‌های رایانش ابر عمومی است.

این استاندارد به‌طور خاص، با در نظر گرفتن الزامات تنظیمی برای حفاظت از PII، راهنماهایی بر اساس استاندارد ISO/IEC 27002 [1] مشخص می‌کند که ممکن است در زمینه‌ی محیط(های) مخاطره‌آمیز امنیت اطلاعات در ارائه‌دهنده‌ی خدمات ابر عمومی قابل‌پذیرش باشند.

این استاندارد برای سازمان‌هایی از هر نوع و با هراندازه، ازجمله شرکت‌های عمومی و خصوصی، هستار[2]های دولتی و سازمان‌های غیرانتفاعی که به‌عنوان پردازشگر PII از طریق رایانش ابری تحت قرارداد با سازمان‌های دیگر، خدمات پردازش اطلاعات ارائه می‌کنند، کاربست‌پذیر است.

همچنین راهنماهای این استاندارد می‌توانند مربوط به سازمان‌هایی باشند که به‌عنوان واپایش‌گران PII عمل می‌کنند؛ بااین‌حال، واپایش‌گران PII ممکن است تحت تأثیر قانون[3]، مقررات و تعهدات افزوده حفاظت از PII قرار گیرند که به پردازشگرهای PII اعمال نمی‌شود. این استاندارد برای پوشش چنین تعهدات افزوده در نظر گرفته نشده است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

---

۱ - استاندارد ملی ایران با شماره ۲۷۰۰۲ ISIRI-ISO/IECدر سال ۱۳۸۷ با منبع بین‌المللی ISO/IEC 27002:2005 منتشر شده است.

2 - Entity

3 - Legislation

2-1 ISO/IEC 17788 | Rec. ITU-T Y.3500, Information technology — Cloud computing — Overview and vocabulary

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سامانه‌های (سیستم-های) مدیریت امنیت اطلاعات مرور کلی و واژگان

۲-۳ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات

۲-۴ استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فن‌آوری اطلاعات - فنون امنیتی -آیین کار مدیریت امنیت اطلاعات

2-5 ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴ و استاندارد ISO/IEC 17788، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

نشت داده

data breach

نقض امنیت است که منجر به تخریب، از دست رفتن، تحریف، افشا یا دسترسی غیرمجاز تصادفی یا غیر-قانونی[1] امنیت که به داده‌های محافظت شده که انتقال می‌یابد، ذخیره می‌شود و یا تحت پردازش قرار می-گیرد.

[منبع: ISO/IEC 27040, 3.7]

۳-۲

اطلاعات قابل‌شناسایی شخصی

personally identifiable information (PII)

هرگونه اطلاعاتی که (الف) بتواند برای شناسایی مالک PII که این اطلاعات به او مربوط می‌شود، استفاده شود یا (ب) پیوند مستقیم یا غیرمستقیم به مالک PII داشته باشد.

یادآوری ۱ مدخل- برای تعیین قابل شناسایی بودن مالک PII، تمام ابزارهایی که به‌طور منطقی برای شناسایی شخص

1 - Unlawful

طبیعی می‌توانند توسط ذینفعان حریم خصوصی که داده‌ها را در اختیار دارند و یا هر شخص دیگری استفاده شوند، باید مورد توجه قرار گیرند.

[منبع: ISO/IEC 29100:2011, 2.9]

یادآوری ۲ مدخل- این تعریف به این منظور آورده شده است تا اصطلاح PII را آن‌گونه که در این استاندارد استفاده می‌شود، تعریف کند. پردازشگر PII ابر عمومی معمولاً در موقعیتی نیست که صراحتاً بداند آیا اطلاعاتی که پردازش می‌کند در دسته مشخصی قرار می‌گیرند یا خیر، مگر اینکه توسط مشتری خدمت ابری شفاف‌سازی شده باشد.

۳-۳

واپایش‌گر PII

PII controller

ذینفع (ذینفعان) حریم خصوصی که مقاصد و ابزارهای پردازش اطلاعات قابل‌شناسایی شخصی (PII) را تعیین می‌کند که با افراد حقیقی که از داده‌ها برای مقاصد شخصی استفاده می‌کنند، متفاوت هستند.

یادآوری ۱- واپایش‌گر PII گاهی از دیگران (به‌عنوان مثال پردازشگر PII) می‌خواهد که از طرف او PII را پردازش کنند درحالی‌که مسئولیت این پردازش با واپایش‌گر PII است.

[منبع: ISO/IEC 29100:2011, 2.10]

۴-۳

مالک PII

PII principal

آدم‌واره‌ای[1] که اطلاعات قابل‌شناسایی شخصی (PII)، مربوط به او است.

یادآوری ۱- بسته به حوزه قضایی و حفاظت خاص از PII و قوانین حریم خصوصی، همچنین واژه مترادف «موضوعِ داده« می‌تواند به‌جای اصطلاح «مالک PII» استفاده شود.

[منبع:ISO/IEC 29100:2011, 2.11]

۵-۳

پردازشگر PII

PII processor

ذینفعان حریم خصوصی که به نمایندگی و مطابق با دستور واپایش‌گر PII، اطلاعات قابل‌شناسایی شخصی (PII) را پردازش می‌کنند.

1 - Natural person

[منبع: ISO/IEC 29100:2011, 2.12]

۶-۳

پردازش PII

processing of PII

عملیات یا مجموعه‌ای از عملیات که روی اطلاعات قابل‌شناسایی شخصی (PII) انجام می‌شود.

یادآوری ۱- نمونه‌هایی از عملیات پردازش PII شامل جمع‌آوری، ذخیره‌سازی، تغییر، بازیابی، مشاوره، افشا، گمنام‌ساز[1]، شبه گمنام‌سازی[2]، انتشار[3] یا در دسترس قرار دادن، حذف یا تخریب PII هستند. البته این عملیات فقط محدود به این موارد نمی‌شود.

[منبع: ISO/IEC 29100:2011, 2.23]

۷-۳

ارائه‌دهنده خدمات ابر عمومی[4]

public cloud service provider

طرفی که با توجه به الگوی ابر عمومی، خدمات ابری را در دسترس قرار می‌دهد.

۴ مرور کلی

۱-۴ ساختار این استاندارد

این استاندارد دارای ساختار شبیه به استاندارد ISO/IEC 27002 است. در مواردی که اهداف و واپایش‌های مشخص شده در استاندارد ISO/IEC 27002 بدون نیاز به هیچ‌گونه اطلاعات افزوده‌ای کاربست‌پذیر هستند، تنها به استاندارد ISO/IEC 27002 ارجاع داده می‌شود. واپایش‌های افزوده و راهنمای پیاده‌سازی مرتبط که در رابطه با حفاظت PII برای ارائه‌دهندگان خدمات رایانش ابری کاربست‌پذیر هستند در پیوست الف (الزامی) شرح داده شده‌اند.

در مواردی که واپایش‌ها برای حفاظت از PII توسط ارائه‌دهندگان خدمات رایانش ابری نیازمند راهنمای کاربست‌پذیر افزوده هستند، این راهنماها تحت عنوان *راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی* آورده شده است. در برخی موارد، اطلاعات مرتبط بیشتر که راهنماهای افزوده را ارتقا می‌دهند، تحت عنوان *اطلاعات دیگر برای حفاظت PII در ابر عمومی* فراهم می‌شوند.

1 - Anonymization
2 - Pseudonymization
3 - Dissemination
4 - Public cloud service provider

همان‌طور که در جدول ۱ نشان داده شده، چنین راهنماها و اطلاعات بخشِ خاص، در رده‌بندی‌های تعریف شده در استاندارد ISO/IEC 27002 قرار می‌گیرند. شماره بندها مطابق با آنچه در جدول نشان داده شده، با شماره بندهای متناظر در استاندارد ISO/IEC 27002 هم‌تراز شده‌اند.

جدول ۱- محل راهنماهای بخش خاص و اطلاعات دیگر برای پیاده‌سازی واپایش در استاندارد ISO/IEC 27002

شماره بند	عنوان	ملاحظات
۵	خط‌مشی‌های امنیت اطلاعات	راهنمای پیاده‌سازی بخش خاص و اطلاعات دیگر ارائه شده است.
۶	سازمان امنیت اطلاعات	راهنمای پیاده‌سازی بخش خاص ارائه شده است.
۷	امنیت منابع انسانی	راهنمای پیاده‌سازی بخش خاص و اطلاعات دیگر ارائه شده است.
۸	مدیریت دارایی	هیچ راهنمای افزوده‌ی پیاده‌سازی بخش خاص و یا اطلاعات دیگر ارائه نشده است.
۹	واپایش دسترسی	راهنمای پیاده‌سازی بخش خاص، همراه با ارجاع به واپایش (ها) در پیوست الف ارائه شده است.
۱۰	رمزنگاری	راهنمای پیاده‌سازی بخش خاص ارائه شده است.
۱۱	امنیت فیزیکی و محیطی	راهنمای پیاده‌سازی بخش خاص، همراه با ارجاع به واپایش (ها) در پیوست الف ارائه شده است.
۱۲	امنیت عملیات	راهنمای پیاده‌سازی بخش خاص ارائه شده است.
۱۳	امنیت ارتباطات	راهنمای پیاده‌سازی بخش خاص، همراه با ارجاع به واپایش (ها) در پیوست الف ارائه شده است.
۱۴	اکتساب، توسعه و نگهداری سامانه	هیچ راهنمای افزوده‌ی پیاده‌سازی بخش خاص و یا اطلاعات دیگر ارائه نشده است.
۱۵	روابط تأمین‌کنندگان	هیچ راهنمای افزوده‌ی پیاده‌سازی بخش خاص و یا اطلاعات دیگر ارائه نشده است.
۱۶	مدیریت رخداد امنیت اطلاعات	راهنمای پیاده‌سازی بخش‌های خاص ارائه شده است.
۱۷	جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار	هیچ راهنمای افزوده‌ی پیاده‌سازی بخش‌های خاص و یا اطلاعات دیگر ارائه شده است.
۱۸	انطباق	راهنمای پیاده‌سازی بخش‌های خاص، همراه با ارجاع به واپایش (بازدید کنندگان) در پیوست الف ارائه شده است.

۲-۴ رده بندی‌های واپایش

در استاندارد ISO/IEC 27002، هر رده اصلی واپایش شامل موارد زیر است:
الف) هدف واپایشی بیان کننده آن چیزی است که قرار است به دست آید؛ و
ب) یک یا چند واپایش که می‌تواند برای رسیدن به اهداف واپایشی استفاده شود.
توصیفات واپایش به‌صورت زیر است:

واپایش

بیانیه خاص واپایش برای برآوردن هدف واپایشی را تعریف می‌کند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

اطلاعات تفصیلی بیشتری برای پشتیبانی از پیاده‌سازی واپایش و دستیابی به اهداف واپایشی فراهم می‌کند. این راهنمایی ممکن است به صورت کامل برای تمامی موقعیت‌ها مناسب و کافی نباشد و ممکن است الزامات واپایشی خاص سازمان را برآورده نسازد. واپایش‌های افزوده و جایگزین، یا قالب‌های دیگر برطرف-سازی مخاطره (اجتناب، انتقال یا پذیرش مخاطره)، ممکن است مناسب باشد.

اطلاعات دیگر برای حفاظت PII در ابر عمومی

اطلاعات بیشتری را که ممکن است نیاز باشد در نظر گرفته شوند، مانند ملاحظات قانونی و ارجاع به استانداردهای دیگر را فراهم می‌کند.

۵ خط‌مشی‌های امنیت اطلاعات

۵-۱ هدایت مدیریت برای امنیت اطلاعات

هدف مشخص شده در بند ۵-۱ از استاندارد ISO/IEC 27002:2013، اعمال می‌شود.

۵-۱-۱ خط‌مشی‌های امنیت اطلاعات

واپایش ۵-۱-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز استفاده می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود خط‌مشی‌های امنیت اطلاعات توسط بیانیه مربوط به حمایت و تعهد جهت دستیابی به سازگاری با قوانین حفاظت PII و شرایط قراردادی مورد توافق بین پردازشگر PII ابر عمومی و مشتریان (مشتریان خدمات ابری) غنی شود.

توصیه می‌شود توافقات قراردادی با در نظر گرفتن نوع خدمات ابری مورد تقاضا (به‌عنوان مثال خدمت از دسته IaaS، PaaS یا SaaS از معماری مرجع رایانش ابری) به‌طور واضح مسئولیت‌های پردازشگر PII ابر عمومی، پیمانکاران و مشتریان خدمت ابری را مشخص نماید. به‌عنوان مثال، تخصیص مسئولیت واپایش لایه‌ی برنامه کاربردی ممکن است بسته به اینکه پردازشگر PII ابر عمومی خدمات IaaS، PaaS یا SaaS که بر اساس آن مشتریان خدمات ابری می‌توانند برنامه‌های کاربردی خود را بسازند و یا لایه‌بندی کنند، ارائه دهد متفاوت باشد.

اطلاعات دیگر برای حفاظت PII در ابر عمومی

در برخی از حوزه‌های قضایی، پردازشگر PII ابر عمومی مستقیماً با قوانین حفاظت PII سروکار دارد. درجاهای دیگر، قانون حفاظت از PII تنها شامل واپایش‌گران PII می‌شود.

سازوکار برای حصول اطمینان از این‌که پردازشگر PII ابر عمومی، متعهد کردن آن به پشتیبانی و مدیریت

انطباق ایجاد شده از طریق قرارداد بین مشتری خدمات ابری و پردازشگر PII ابـر عمـومی فـراهم مـی‌شـود. قرارداد می‌تواند انطباق ممیزی‌شده‌ی مستقل که مورد قبول مشـتری خـدمت ابـر اسـت را در نظـر بگیـرد، به‌عنوان مثال از طریق پیاده‌سازی واپایش‌های مربوط در این استاندارد و در استاندارد ISO/IEC 27002.

۵-۱-۲ بازنگری خط‌مشی‌های امنیت اطلاعات

واپایش ۵-۱-۲ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۶ سازمان امنیت اطلاعات

۶-۱ سازمان داخلی

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 6.1 به‌کار می‌رود.

۶-۱-۱ نقش‌ها و مسئولیت‌های امنیت اطلاعات

واپایش ۶-۱-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در اسـتاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز به کار می‌رود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود پردازشگر PII ابر عمومی، در رابطه با پردازش PII تحت قرارداد، رابط کمیسیون برای مشتری خدمات ابری تعیین کند.

۶-۱-۲ تفکیک وظایف

واپایش ۶-۱-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در اسـتاندارد ISO/IEC 27002 اعمال می‌شود.

۶-۱-۳ برقراری ارتباط با مراجع دارای اختیار [1]

واپایش ۶-۱-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در اسـتاندارد ISO/IEC 27002 اعمال می‌شود.

۶-۱-۴ برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص [2]

واپایش ۶-۱-۴ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در اسـتاندارد ISO/IEC 27002 اعمال می‌شود.

1- Contact with authorities
2- Special interest groups

۶-۱-۵ امنیت اطلاعات در مدیریت پروژه

واپایش ۶-۱-۵ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۶-۲ افزاره‌های سیار[1] و دورکاری

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 6.2 اعمال می‌شود.

۷ امنیت منابع انسانی

۷-۱ پیش از اشتغال[2]

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 7.1 اعمال می‌شود.

۷-۲ در حین خدمت

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 7.2 اعمال می‌شود.

۷-۲-۱ مسئولیت‌های مدیریت

واپایش ۷-۲-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۷-۲-۲ آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات

واپایش ۷-۲-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود اقدامات در محلی متمرکز شود تا اعضاء مرتبط به‌ویژه آن‌ها که به اداره PII می‌پردازند، از نتایج احتمالی نقض حریم خصوصی یا روش قوانین امنیتی، بر پردازشگر PII ابر عمومی (به‌عنوان مثال عواقب قانونی، زیان کار و نام تجاری یا آسیب اعتباری)، بر کارکنان (به‌عنوان مثال عواقب انضباطی) و بر مالک PII (به‌عنوان مثال عواقب فیزیکی، مادی و عاطفی) آگاه شوند.

اطلاعات دیگر برای حفاظت PII در ابر عمومی

در برخی از حوزه‌های قضایی، پردازشگر PII ابر عمومی ممکن است در معرض تحریم‌های قانونی، ازجمله جریمه قابل‌توجه مستقیماً از مسئول محلی حفاظت PII قرار بگیرد. در سایر حوزه‌های قضایی استفاده از استانداردهای ملی مانند این در تنظیم قرارداد بین پردازشگر PII ابر عمومی و مشتری خدمت ابری، باید به

1- Mobile devices
2- Employment

ایجاد اصولی برای تحریم قراردادهای با هدف نقض قوانین و روش‌های امنیتی کمک کند.

۷-۲-۳ فرآیند انضباطی

واپایش ۷-۲-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۷-۳ خاتمه و تغییر استخدام

محتویات و هدف مشخص شده در بند ۷-۳ از استاندارد ISO/IEC 27002:2013 اعمال می‌شود.

۸ مدیریت دارایی

محتویات و اهداف مشخص شده در بند ۸ از استاندارد ISO/IEC 27002:2013 اعمال می‌شود.

۹ واپایش دسترسی

۹-۱ الزامات کسب‌وکار واپایش دسترسی

محتویات و اهداف مشخص شده در بند ۹-۱ از استاندارد ISO/IEC 27002:2013 اعمال می‌شود.

۹-۲ مدیریت دسترسی کاربر

هدف مشخص شده در بند ۹-۲ از استاندارد ISO/IEC 27002:2013 اعمال می‌شود. راهنمای بخش خاص زیر نیز برای پیاده‌سازی تمام واپایش‌ها تحت این بند (۹-۲) اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

در زمینه دسته خدمات معماری مرجع رایانش ابری، مشتری خدمات ابری ممکن است مسئول برخی یا تمام جنبه‌های مدیریت دسترسی کاربران خدمت ابری تحت واپایش باشد. توصیه می‌شود هرکجا مناسب است، پردازشگر PII ابر عمومی، به‌عنوان مثال توسط فراهم آوردن حقوق اداری برای مدیریت و یا فسخ دسترسی، مشتری خدمات ابری را به مدیریت دسترسی کاربران خدمت ابری تحت واپایش مشتریان خدمات ابری قادر سازد.

۹-۲-۱ ثبت‌نام و لغو ثبت‌نام[1]

واپایش ۹-۲-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

2- De-registration

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود رویه‌های ثبت‌نام و لغو ثبت‌نام کاربر، به وضعیتی که در آن واپایش دسترسی کاربر از دست رفته است ، مانند خراب شدن و یا توافق روی گذر واژه‌ها یا دیگر اطلاعاتِ ثبت‌نامی کاربر (به‌عنوان مثال درنتیجه افشای غیرعمدی) بپردازد.

یادآوری- هر یک از حوزه‌های قضایی ممکن است الزامات خاصی را در مورد بسامد وارسی‌ها برای اعتبارنامه‌های اصالت‌سنجیِ استفاده نشده تحمیل کند. توصیه می‌شود سازمان‌های فعال در این حوزه‌های قضایی اطمینان حاصل کنند که با این شرایط تطابق داشته باشند.

۹-۲-۲ تأمین دسترسی کاربر

واپایش ۹-۲-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۲-۳ مدیریت حقوق ویژه[1] دسترسی

واپایش ۹-۲-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۲-۴ مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران

واپایش ۹-۲-۴ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۲-۵ بازنگری حقوق دسترسی کاربر

واپایش ۹-۲-۵ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۲-۶ حذف و یا تنظیم حقوق دسترسی

واپایش ۹-۲-۶ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۳ مسئولیت‌های کاربر

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 9.3 اعمال می‌شود.

۹-۳-۱ استفاده از اطلاعات اصالت‌سنجی مخفی

واپایش ۹-۳-۱ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

1- Privileged

۹-۴ واپایش دسترسی به سامانه‌ها و برنامه‌های کاربردی

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 9.4 اعمال می‌شود.

۹-۴-۱ محدودسازی دسترسی به اطلاعات

واپایش ۹-۴-۱ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

یادآوری- راهنماها و واپایش‌های افزوده مربوطه به محدود کردن دسترسی به اطلاعات را می‌توان در الف-۱۰-۱۳ پیدا کرد.

۹-۴-۲ روش‌های اجرایی ورود امن

واپایش ۹-۴-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود هر جا که لازم باشد، پردازشگر PII ابر عمومی روش امن ورود به سامانه برای هر اشتراک درخواست شده توسط مشتری خدمت ابری تحت واپایش کاربران خدمات ابری فراهم کند.

۹-۴-۳ سامانه مدیریت گذر واژه

واپایش ۹-۴-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۴-۴ استفاده از برنامه‌های کمکی ویژه

واپایش ۹-۴-۴ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۹-۴-۵ واپایش دسترسی به کد منبع برنامه

واپایش ۹-۴-۵ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۰ رمزنگاری

۱۰-۱ واپایش‌های رمزنگاری

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 10.1 اعمال می‌شود.

۱۰-۱-۱ خط‌مشی استفاده از واپایش‌های رمزنگاری

واپایش ۱۰-۱-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود پردازشگر PII ابر عمومی با توجه به شرایط استفاده از رمزنگاری برای حافظت از PII در حال پردازش، اطلاعات درخواست شده مشتری خدمت ابری را فراهم کند. همچنین توصیه می‌شود پردازشگر PII ابر عمومی در مورد تمام قابلیت‌هایش که ممکن است برای اعمال حفاظت رمزنگاری به مشتری خدمات ابری کمک کند، اطلاعات مورد نیاز مشتری خدمت ابری را فراهم کند.

یادآوری- در برخی حوزه‌های قضایی ممکن است برای حفاظت از انواع خاصی از PII، رمز لازم باشد، مانند داده‌های مربوط به سلامتی، شماره‌های ثبت اقامت، شماره گذرنامه و شماره گواهینامه رانندگی مربوط به مالک PII.

۱۰-۱-۲ مدیریت کلید

واپایش ۱۰-۱-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱ امنیت فیزیکی و محیطی

۱۱-۱ نواحی امن

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 11.1 اعمال می‌شود.

۱۱-۲ تجهیزات

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 11.2 اعمال می‌شود.

۱۱-۲-۱ استقرار و حفاظت تجهیزات

واپایش ۱۱-۲-۱ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۲ ابزارهای پشتیبانی[1]

۱۱-۲-۲ واپایش و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۳ امنیت کابل‌کشی

۱۱-۲-۳ واپایش و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

1- Supporting Utilities

۱۱-۲-۴ نگهداری تجهیزات

واپایش ۱۱-۲-۴ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۵ خروج دارایی

واپایش ۱۱-۲-۵ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۶ امنیت تجهیزات خارج از محوطه[1]

واپایش ۱۱-۲-۶ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۷ امحاء یا استفاده مجدد امن از تجهیزات

واپایش ۱۱-۲-۷ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش- خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی ابر عمومی حفاظت PII

توصیه می‌شود به منظور دسترسی امن و یا استفاده مجدد، تجهیزات شامل رسانه‌های ذخیره‌سازی که ممکن است شامل PII باشند همان‌طور که هستند مورد استفاده قرار بگیرند.

یادآوری- راهنماها و واپایش‌های افزوده مربوط به دسترسی امن و یا استفاده مجدد از تجهیزات را می‌توان در الف-۱۰-۱۳ پیدا کرد.

۱۱-۲-۸ تجهیزات بدون مراقبت کاربر

واپایش ۱۱-۲-۸ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۱-۲-۹ خط‌مشی میز پاک و صفحه پاک

واپایش ۱۱-۲-۹ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۲ امنیت عملیات

۱۲-۱ مسئولیت‌ها و روش‌های اجرایی عملیاتی

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.1 اعمال می‌شود.

1- Premises

۱-۱-۱۲ روش‌های اجرایی عملیاتی مستند

واپایش ۱-۱-۱۲ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۲-۱-۱۲ مدیریت تغییر

واپایش ۲-۱-۱۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۳-۱-۱۲ مدیریت ظرفیت

۳-۱-۱۲ واپایش و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۴-۱-۱۲ جداسازی محیط توسعه، آزمون و عملیاتی

۴-۱-۱۲ واپایش و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود جایی که استفاده از PII برای رسیدن به هدف آزمایش، اجتناب‌ناپذیر است، ابتدا ارزیابی مخاطره انجام شود. اقدامات فنی و سازمانی برای به کمینه رساندن مخاطرات شناسایی‌شده باید اجرا شوند.

۲-۱۲ حفاظت در برابر بدافزار

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.2 اعمال می‌شود.

۳-۱۲ نسخه‌های پشتیبان

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.3 اعمال می‌شود.

۱-۳-۱۲ ایجاد پشتیبان از اطلاعات

واپایش ۱-۳-۱۲ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

سامانه‌های پردازش اطلاعات بر اساس الگوی رایانش ابری، سازوکار افزوده یا جایگزین برای پشتیبان‌گیری خارج از سایت جهت حافظت در برابر زیان داده‌ها، حصول اطمینان از تداوم عملیات پردازش داده‌ها و توانایی بازگرداندن عملیات پردازش داده‌ها پس از اتفاق مخرب معرفی می‌کنند. توصیه می‌شود به منظور پشتیبان-گیری و یا بازگرداندن اطلاعات، نسخه‌های متعدد داده‌ها در مکان‌های مختلف از نظر فیزیکی یا منطقی (که ممکن است در خود سامانه پردازش اطلاعات باشد) ایجاد شده و یا حفظ شود.

ممکن است مسئولیت‌های خاص PII نسبت به مشتری خدمت ابری در این رابطه نهفته باشد. توصیه می‌شود هر جا که پردازشگر PII ابر عمومی صراحتاً خدمات پشتیبان‌گیری و بازیابی برای مشتریان خدمات ابری فراهم می‌کند، پردازشگر PII ابر عمومی اطلاعات شفافی در رابطه با قابلیت پشتیبان‌گیری و ذخیره مجدد داده‌ها، به مشتری خدمت ابری ارائه دهد.

یادآوری ۱- حوزه‌های خاص ممکن است الزامات خاصی در رابطه با بسامد پشتیبان‌گیری را تحمیل کنند. توصیه می‌شود سازمان‌های فعال در این حوزه‌ها اطمینان حاصل کنند که با این الزامات موافق هستند. همچنین توصیه می‌شود روش‌های پیاده‌سازی طی یک دوره مستند و مشخص پس از فرایندی مخرب، جمع‌آوری شوند تا اجازه ذخیره مجدد عملیات پردازش داده‌ها را بدهند.

توصیه می‌شود فرایندهای پشتیبان‌گیری و بازیابی در یک بسامد مشخص مستندسازی تجدید شود.

یادآوری ۲- حوزه‌های خاص ممکن است الزامات خاصی را از نظر بسامد تجدید فرایند پشتیبان‌گیری و بازیابی تحمیل کنند. سازمان‌های فعال در این حوزه‌های باید اطمینان حاصل کنند که با این الزامات موافق هستند.

استفاده از پیمانکاران جزء برای ذخیره و یا کپی نسخه پشتیبان داده‌های در حال پردازش، توسط واپایش‌ها در این استاندارد مورد استفاده برای پردازش PII تحت قرارداد پوشش داده می‌شود. همچنین هر جا انتقال رسانه فیزیکی رخ دهد توسط واپایش‌های این استاندارد پوشش داده می‌شود.
توصیه می‌شود پردازشگر PII ابر عمومی خط‌مشی جهت پرداختن به الزامات پشتیبان‌گیری از اطلاعات و هرگونه الزامات بیشتر (به‌عنوان مثال الزامات قراردادی و یا حقوقی) برای پاک کردن PII موجود در اطلاعات حفظ شده به منظور پشتیبان‌گیری داشته باشد.

۱۲-۴ واقعه‌نگاری و پایش

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.4 اعمال می‌شود.

۱۲-۴-۱ واقعه‌نگاری رویداد

واپایش ۱۲-۴-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود به منظور شناسایی بی‌نظمی‌ها و پیشنهاد تلاش‌های اصلاحی، روند روی بررسی ثبت رویدادها طی دوره تناوب مستند و مشخص متمرکز شود.
توصیه می‌شود در صورت امکان، ثبت شود که آیا PII درنتیجه رویداد تغییر کرده است (اضافه، اصلاح و یا حذف شده است) یا نه و اگر تغییر کرده توسط چه کسی بوده است. جایی که ارائه دهندگان خدمات چندگانه درگیر ارائه خدمات از دسته‌های مختلف معماری مرجع رایانش ابری هستند، ممکن است نقش‌ها در این راهنمای پیاده‌سازی متفاوت شده یا مشترک شوند.

توصیه می‌شود پردازشگر PII ابر عمومی محدوده اینکه چه زمانی و چگونه اطلاعات ورود به سامانه می‌تواند توسط مشتری خدمت ابری در دسترس و یا مورد استفاده قرار بگیرد را معین کند. این روش‌ها باید برای مشتری خدمت ابری موجود باشند.

جایی که مشتری خدمت ابری مجاز به دسترسی به سوابق ورود واپایش شده توسط پردازشگر PII ابر عمومی است، توصیه می‌شود پردازشگر PII ابر عمومی اطمینان حاصل کند که مشتری تنها به سوابق مربوط به فعالیت‌های خودش می‌تواند دسترسی پیدا کند، و نه به سوابق فعالیت‌های ثبت شده سایر مشتریان.

۱۲-۴-۲ حفاظت از اطلاعات ثبت‌شده وقایع

واپایش ۱۲-۴-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی خاص حفاظت ابر عمومی PII

اطلاعات ورود ثبت شده ممکن است برای اهدافی مانند نظارت بر امنیت و تشخیص‌های عملیاتی شامل PII شوند. توصیه می‌شود اقداماتی مانند واپایش دسترسی (نگاه کنید به ۹-۲-۳)، متمرکز شوند تا اطمینان حاصل شود که اطلاعات ورود تنها برای اهداف در نظر گرفته شده به‌کار می‌روند. توصیه می‌شود یک روش، ترجیحاً خودکار، در نظرگرفته شود تا اطمینان حاصل شود که اطلاعات ورود طی یک دوره مشخص و مستند حذف می‌شوند.

۱۲-۴-۳ ثبت وقایع سرپرست و بهره‌بردار سیستم

واپایش ۱۲-۴-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۲-۴-۴ هم‌زمان‌سازی ساعت‌ها

واپایش ۱۲-۴-۴ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۲-۵ واپایش نرم‌افزارهای عملیاتی

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.5 اعمال می‌شود.

۱۲-۶ مدیریت آسیب‌پذیری فنی

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.6 اعمال می‌شود.

۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 12.7 اعمال می‌شود.

۱۳ امنیت ارتباطات

۱-۱۳ مدیریت امنیت شبکه

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 13.1 اعمال می‌شود.

۲-۱۳ انتقال اطلاعات

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 13.2 اعمال می‌شود.

۱-۲-۱۳ خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات

واپایش ۱۳-۲-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز اعمال می‌شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود هر زمان که محیط فیزیکی برای انتقال اطلاعات استفاده شود، سامانه برای ضبط محیط‌های فیزیکی ورودی و خروجی حاوی PII شامل نوع محیط فیزیکی، فرستنده / گیرنده مجاز، تاریخ و زمان و تعداد محیط‌های فیزیکی در نظر گرفته شود. در صورت امکان، در رابطه با اقدامات افزوده (مانند رمزنگاری) از مشتریان خدمات ابری نظرخواهی شود تا اطمینان حاصل شود که داده‌ها تنها می‌تواند در نقطه مقصد در دسترس باشند و نه در حین مسیر.

۲-۲-۱۳ توافق‌نامه‌های انتقال اطلاعات

واپایش ۱۳-۲-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۳-۲-۱۳ پیام‌رسانی الکترونیکی

واپایش ۱۳-۲-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۴-۲-۱۳ توافق‌نامه‌های محرمانگی یا عدم افشاء

واپایش ۱۳-۲-۴ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

یادآوری- راهنماها واپایش‌های افزوده مربوط به توافق‌های محرمانه بودن یا عدم افشا می‌تواند در الف-۱۰-۱ یافت شود.

۱۴ اکتساب، توسعه و نگهداری سامانه

محتویات و اهداف مشخص شده در استاندارد ISO/IEC 27002:2013، بند ۱۴ اعمال می‌شود.

۱۵ ارتباط با تأمین‌کنندگان

محتویات و اهداف مشخص شده در استاندارد ISO/IEC 27002:2013، بند ۱۵ اعمال می‌شود.

یادآوری- اطلاعات بیشتر در مورد مدیریت تأمین‌کننده روابط ممکن است از ISO/IEC 27036-4 به دست آید.

۱۶ مدیریت رخداد امنیت اطلاعات

۱-۱۶ مدیریت رخدادهای امنیت اطلاعات و بهبودها

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 16.1 اعمال می‌شود. راهنمای بخش خاص زیر نیز برای پیاده‌سازی تمام واپایش تحت این بند (۱-۱۶) به‌کار می‌رود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

در زمینه تمام معماری مرجع رایانش ابری ممکن است نقش‌های مشترکی در بهبود و مدیریت رویدادهای امنیت اطلاعات وجود داشته باشد. ممکن است در پیاده‌سازی واپایش‌های این بند پردازشگر PII ابر عمومی نیاز به همکاری با مشتری خدمات ابری داشته باشد.

۱-۱-۱۶ مسئولیت‌ها و روش‌های اجرایی

واپایش ۱-۱-۱۶ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

به‌عنوان بخشی از فرآیند مدیریت رویداد امنیت اطلاعات، برای تعیین اینکه آیا نقض داده‌های متعلق به PII صورت گرفته یا خیر، بررسی‌هایی توسط پردازشگر PII ابر عمومی در رویداد امنیت اطلاعات آغاز می‌شود (به الف-۹-۱ مراجعه شود).

رویداد امنیت اطلاعات نباید لزوماً منجر به چنین بررسی شود. رویدادی امنیت اطلاعاتی است که با احتمال بالایی منتج به دسترسی غیرمجاز و بدون محدودیت به PII یا هر یک از الزامات پردازشگر PII ابر عمومی و یا امکانات ذخیره‌سازی PII شود که ممکن است شامل پینگ[1]ها و سایر حملات گسترده به دیوارهای آتش یا کارسازها، پویش درگاه‌ها تلاش ناموفق ورود به سامانه، حملات انکار خدمت (حملات DoS) و پویشگر است، نشود.

1- Ping

۱۶-۱-۲ گزارش‌دهی رویدادهای امنیت اطلاعات

واپایش ۱۶-۱-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۶-۱-۳ گزارش دهی ضعف‌های امنیتی

واپایش ۱۶-۱-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۶-۱-۴ ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات

واپایش ۱۶-۱-۴ و راهنمای پیاده‌سازی مرتبط مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۶-۱-۵ پاسخ به رخدادهای امنیت اطلاعات

واپایش ۱۶-۱-۵ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۶-۱-۶ یادگیری از رخدادهای امنیت اطلاعات

واپایش ۱۶-۱-۶ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۶-۱-۷ جمع‌آوری شواهد

واپایش ۱۶-۱-۷ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار

محتویات و اهداف مشخص شده در استاندارد ISO/IEC 27002:2013، بند ۱۷ اعمال می‌شود.

۱۸ انطباق

۱۸-۱ انطباق با الزامات قانونی و قراردادی

محتویات و هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 18.1 اعمال می‌شود.

یادآوری- واپایش‌ها و راهنماهای افزوده مربوط به انطباق با الزامات قانونی و قراردادی می‌تواند در بند الف-۱۱ یافت شود.

۱۸-۲ بازنگری‌های امنیت اطلاعات

هدف مشخص شده در استاندارد ISO/IEC 27002:2013, 18.2 اعمال می‌شود.

۱۸-۲-۱ بازنگری مستقل امنیت اطلاعات

واپایش ۱۸-۲-۱ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود در مواردی که حسابرسی مشتری خدمات ابری خاصی غیرعملی باشد یا خطراتی برای امنیت داشته باشد (مراجعه شود به بند ۱۰-۰)، پردازشگر PII ابر عمومی قبل از ورود به قرارداد و در طول مدت زمان قرارداد، شواهد مستقلی مبنی بر اجرا و راه‌اندازی امنیت اطلاعات مطابق خط مش‌ها و روش‌های پردازشگر PII ابر عمومی در دسترس مشتریان خدمات ابری قرار دهد. حسابرسی مستقل مربوطه مطابق آنچه توسط پردازشگر PII ابر عمومی انتخاب می‌شود، معمولاً باید روش قابل قبول برای انجام خواسته‌های مشتریان خدمات ابری در بررسی عملیات پردازش پردازشگر PII ابر عمومی باشد که شفافیت کافی نیز ارائه شده باشد.

۱۸-۲-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

واپایش ۱۸-۲-۲ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

۱۸-۲-۳ بازنگری انطباق فنی

واپایش ۱۸-۲-۳ و راهنمای پیاده‌سازی مرتبط و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 اعمال می‌شود.

پیوست الف

(الزامی)

مجموعه واپایش‌های توسعه‌یافته برای حفاظت پردازشگر PII ابر عمومی

این پیوست واپایش‌های جدید و راهنماهای پیاده‌سازی مرتبط با آن‌ها را مشخص می‌کند که در ترکیب با واپایش‌ها و راهنماهای اضافه در استاندارد ISO/IEC 27002 (به بند ۵-۱۸ مراجعه شود)، مجموعه گسترده واپایش‌ها را می‌سازد که توسط ارائه‌کنندگان خدمات ابر عمومی که به‌عنوان پردازشگر PII عمل می‌کنند برای رسیدن به الزامات حفاظت PII به‌کار می‌رود.

این واپایش‌های افزوده با توجه به ۱۱ اصل حفظ حریم خصوصی ISO/IEC 29100 طبقه‌بندی می‌شوند. در بسیاری موارد واپایش‌ها می‌توانند توسط بیش از یکی از اصول حفظ حریم خصوصی طبقه‌بندی شوند. در چنین مواردی با توجه به مناسب‌ترین اصل، طبقه بندی انجام می‌شود.

الف-۱ رضایت[1] و انتخاب[2]

الف-۱-۱ تعهد به همکاری در رابطه با حقوق مدیران PII،

واپایش

توصیه می‌شود پردازشگر PII ابر عمومی مشتریان را قادر به انجام التزاماتشان به منظور تسهیل در اعمال حقوق مدیران PII سازد تا دسترسی، تصحیح و یا پاک کردن PII مربوطشان را فراهم کند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

التزامات واپایش‌گر PII در این رابطه توسط قانون، مقررات یا قرارداد تعریف شده است.

این التزامات ممکن است شامل مسائلی مثل اصلاح یا حذف به موقع PII باشند که مشتری خدمات ابری برای پیاده‌سازی خدمات پردازشگر PII ابر عمومی استفاده می‌کند.

هر جا که واپایش‌گر PII برای اطلاعات و یا اقدامات فنی جهت تسهیل در اعمال حقوق مدیران PII وابسته به پردازشگر PII ابر عمومی است، اطلاعات مربوطه و یا اقدامات فنی باید در قرارداد مشخص شده باشند.

1- Consent
2- Choice

الف-۲ مشروعیت هدف و مشخصات

الف-۲-۱ هدف پردازشگر PII ابر عمومی

واپایش

توصیه نمی‌شود PII که قرار است تحت قرارداد پردازش شود، برای هیچ هدفی به جز دستورالعمل‌های مشتری خدمات ابری پردازش شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

دستورالعمل می‌تواند شامل قرارداد بین پردازشگر PII ابر عمومی و مشتریان خدمات ابری شود مثل هدف و چارچوب زمانی که باید توسط خدمات حاصل شود. به منظور دستیابی به اهداف مشتری خدمات ابری، دلایل فنی ممکن است وجود داشته باشد که چرا برای پردازشگر PII ابر عمومی مناسب است که مطابق با دستورالعمل‌های عمومی مشتری، ولی بدون دستور بیان مشتری، روشی برای پردازش PII تعیین کند. به‌عنوان مثال، به منظور استفاده مؤثر از شبکه و یا ظرفیت پردازش ممکن است تخصیص منابع پردازش خاص بسته به ویژگی‌های خاصی از مالک PII لازم باشد. در چنین شرایطی تعیین پردازشگر PII ابر عمومی از اصول پردازش حفظ حریم خصوصی مندرج در استاندارد ISO/IEC 29100 تنظیم شده است.

پردازشگر PII ابر عمومی باید به موقع تمام اطلاعات مربوطه برای مشتری خدمات ابری را فراهم کند تا به وی اجازه دهد که از توافق پردازشگر PII ابر عمومی با مشخصات هدف و اصول محدودیت و اینکه هیچ PII توسط پردازشگر PII ابر عمومی یا هر یک از پیمانکاران جزء آن برای اهداف بیشتر و جدای از دستورالعمل‌های مشتری پردازش نمی‌شود، اطمینان حاصل کند.

الف-۲-۲ استفاده تجاری پردازشگر PII ابر عمومی

واپایش

توصیه نمی‌شود PII که قرار است تحت قرارداد پردازش شود، برای اهداف بازاریابی و تبلیغات بدون رضایت مشتری توسط پردازشگر PII ابر عمومی استفاده شود. چنین رضایتی نباید شرط دریافت این‌گونه خدمات باشد.

یادآوری- این واپایش مازاد بر واپایش کلی‌تر در الف-۲-۱ بوده و جایگزین آن نیست.

الف-۳ محدودیت مجموعه

واپایش افزوده در رابطه با این اصل از حفظ حریم خصوصی وجود ندارد.

الف-۴ به کمینه رساندن داده‌ها

الف-۴-۱ پاک کردن امن پرونده‌های موقت

واپایش

توصیه می‌شود اسناد و پرونده‌های موقت طی دوره مستند مشخص پاک یا نابود شوند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

راهنمای پیاده‌سازی پاک کردن PII در الف-۱۰-۱۱ ارائه شده است.

سامانه‌های اطلاعات در دوره عادی عملکردشان ممکن است پرونده‌های موقت ایجاد کنند. چنین پرونده-هایی مختص هر سامانه یا نرم‌افزاری بوده اما ممکن است نسخه‌های قبلی پرونده‌های سامانه، پرونده‌های موقت متعلق به به‌روزرسانی پایگاه داده‌ها و عملکرد سایر نرم‌افزارهای کاربردی را شامل شوند. پرونده‌های موقت بعد از تکمیل عمل پردازش اطلاعات مرتبط، موردنیاز نیستند اما شرایطی وجود دارد که تحت آن ممکن است این پرونده‌ها حذف نشوند. دوره زمانی که این پرونده‌ها به‌منظور استفاده باقی‌مانده و حذف نمی‌شوند همیشه قطعی نیست، اما رویه‌ی «جمع‌آوری پسماند[1]»، پرونده‌های مربوطه را شناسایی کرده و تعیین می‌کند چه مدتی از آخرین زمان استفاده آن‌ها می‌گذرد. توصیه می‌شود سامانه‌های پردازش PII به‌صورت دوره‌ای وارسی کنند تا پرونده‌های بلااستفاده و موقت با طول عمری بیشتر از یک مقدار مشخص، حذف شوند.

الف-۵ محدودیت استفاده، حفظ و افشاگری

الف-۵-۱ اطلاع‌رسانی افشای PII

واپایش

توصیه می‌شود قرارداد بین پردازشگر PII ابر عمومی و مشتری خدمات ابری، پردازشگر PII ابر عمومی را ملزم کند که مطابق با هر روش و دوره زمانی توافق شده در قرارداد، نسبت به هر درخواست قانونی الزام‌آور برای افشای PII توسط یک مقام پیاده‌سازی قانونی اطلاع‌رسانی به مشتری انجام شود، مگر اینکه چنین افشاگری ممنوع باشد.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود پردازشگر PII ابر عمومی تضمین‌های قراردادی برای موارد زیر فراهم کند: رد هرگونه درخواست برای افشای PII که ازلحاظ قانونی الزام‌آور نیستند، مشورت با مشتری مربوطه در مواردی که ازلحاظ قانونی مجاز است، قبل از هرگونه افشای PII و پذیرفتن هرگونه درخواست مورد توافق در قرارداد برای افشای PII که از نظر مشتری مربوطه مجاز هستند.

1- Garbage collection

یک نمونه‌ای از موارد ممنوعیت افشاگری، ممنوعیت تحت قانون جزائی برای حفظ محرمانه بودن بررسی اجرای قانون است.

الف-۵-۲ ثبت افشای PII

واپایش

توصیه می‌شود افشای PII به اشخاص ثالث، شامل چیزی که PII افشا کرده، به چه کسی و در چه زمانی افشا شده، ثبت شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

ممکن است PII در طول دوره عملکردهای عادی افشا شود. این افشاگری‌ها باید ثبت شود (مراجعه شود به ۱۲-۴-۱). توصیه می‌شود هر افشاگری اضافی به اشخاص ثالث، مثل مواردی که ناشی از تحقیقات قانونی و یا حسابرسی‌های خارجی هستند، نیز ثبت شود. سوابق باید شامل منبع افشاگری‌ها و منبع اختیار افشاگری باشند.

الف-۶ دقت و کیفیت

واپایش افزوده در رابطه با این اصل حفظ حریم خصوصی وجود ندارد.

الف-۷ باز بودن، شفافیت[1] و توجه[2]

الف-۷-۱ افشای پردازش PII تحت قرارداد

واپایش

توصیه می‌شود استفاده از پیمانکاران فرعی توسط پردازشگر PII ابر عمومی برای پردازش PII به مشتریان مربوطه، قبل از استفاده از آن‌ها افشا شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود مقررات استفاده از پیمانکاران فرعی برای پردازش PII در قرارداد بین پردازشگر PII ابر عمومی و مشتری خدمات ابری شفاف باشند. این قرارداد باید مشخص کند که پیمانکاران فرعی ممکن است تنها بر اساس رضایت مشتری در ابتدای درخواستش برای خدمات ابری به‌کار روند. پردازشگر PII ابر عمومی باید به موقع مشتری خدمات ابری را از هرگونه تغییر در نظر گرفته شده در این زمینه آگاه سازند، طوری که مشتری خدمات ابری که امکان اعتراض نسبت به این تغییرات و یا فسخ قرارداد را داشته باشد.

توصیه می‌شود اطلاعات افشا شده نام پیمانکاران مربوطه و این واقعیت که پیمانکاری فرعی به‌کاررفته را پنهان کنند، اما نه هرگونه جزئیات خاص کسب‌وکار را. همچنین اطلاعات افشا شده باید شامل کشورهایی که در آن پیمانکاران فرعی داده‌ها را پردازش کنند (به الف-۱۱-۱ مراجعه شود) و وسایلی که توسط آن‌ها

1- Transparency
2- Notice

پیمانکاران فرعی موظف به رعایت و یا عبور از التزامات پردازشگر PII ابر عمومی هستند (به الف-۱۰-۱۲ مراجعه شود) باشد.
در مواردی که افشای عمومی اطلاعات پیمانکاران فرعی به دلیل افزایش مخاطره امنیتی نسبت به حد قابل قبول مورد توجه قرار گیرد، افشاگری باید تحت یک توافقنامه عدم افشا و یا بر اساس درخواست مشتری خدمات ابری انجام شود. مشتری خدمات ابری باید بداند که اطلاعات موجود هستند.

الف-۸ دسترسی و مشارکت فردی

واپایش‌های افزوده مربوط به این اصل از حفظ حریم خصوصی وجود ندارد.

الف-۹ پاسخگویی

الف-۹-۱ هشدار نقض اطلاعات مربوط PII

واپایش
توصیه می‌شود پردازشگر PII ابر عمومی در صورت هرگونه دسترسی غیرمجاز به PII و یا به تجهیزات یا امکانات پردازش و در نتیجه زیان، فاش شدن و تغییر PII، به سرعت به مشتری خدمات ابری مربوطه اطلاع دهد.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی
مقررات مربوط به اطلاع‌رسانی نقض داده‌های PII باید بخشی از قرارداد بین پردازشگر PII ابر عمومی و مشتری خدمات ابری را تشکیل دهد. قرارداد باید چگونگی فراهم کردن اطلاعات مورد نیاز مشتری توسط پردازشگر PII ابر عمومی جهت انجام تعهدش برای اطلاع‌رسانی به مقامات مربوطه را مشخص کند.
این تعهد اطلاع‌رسانی شامل نقض داده‌های ایجاد شده توسط مشتری خدمات ابری و یا مالک PII یا از طریق اجزای سامانه که مسئول آن‌ها هستند، نمی‌شود. این قرارداد همچنین باید بیشینه تأخیر در اطلاع‌رسانی یک نقض داده PII را تعریف کند.
درصورتی‌که نقض داده شامل PII رخ دهد، باید یک رکورد شامل شرحی از رویداد، دوره زمانی، عواقب ناشی از این رویداد، نام خبرنگاری که این رویداد به وی گزارش شده، اقدامات انجام شده برای حل‌وفصل این رویداد (از جمله فرد مسئول و داده‌های بازیابی شده) و این که آیا این رویداد منجر به زیان، افشا یا تغییر PII شده است یا خیر، حفظ شود.
همچنین توصیه می‌شود در مواردی که نقض داده شامل PII رخ دهد، سوابق شامل شرح داده به خطر افتاده، در صورت شناخته شدن و در صورت انجام اطلاع‌رسانی، اقدامات انجام شده جهت اطلاع مشتری خدمات ابری و یا نمایندگی‌های نظارتی است.

در برخی از حوزه‌ها، قانون یا مقررات مربوط ممکن است پردازشگر PII ابر عمومی نیاز به اطلاع‌رسانی به طور مستقیم به مقامات نظارتی مناسب (به‌عنوان مثال سازمان حفاظت PII) جهت نقض اطلاعات مربوط PII داشته باشد.

یادآوری- ممکن است نقض‌های دیگری که نیاز به اطلاع‌رسانی دارند و در اینجا تحت بررسی قرار نگرفته‌اند وجود داشته باشند، به‌عنوان مثال گردآوری بدون رضایت یا مجوز که برای اهداف غیر قانونی استفاده شود و غیره.

الف-۹-۲ دستورالعمل و دوره حفظ برای خط‌مشی‌های امنیتی اداری

واپایش

توصیه می‌شود نسخه‌هایی از خط‌مشی‌های امنیتی و روش‌های عملیاتی برای یک دوره مشخص مستند از طریق جایگزینی (از جمله به‌روزرسانی) باقی بماند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

ممکن است به‌عنوان مثال در موارد حل اختلاف با مشتری و بررسی توسط یک مقام حفاظت PII، بررسی خط‌مشی‌های گذشته و رویه کنونی نیاز باشد؛ بنابراین توصیه می‌شود یک کمینه دوره بازماندن ۵ ساله در غیاب الزام قانونی یا قراردادی خاص، در نظر گرفته شود.

الف-۹-۳ بازیابی، انتقال و افشای PII

واپایش

توصیه می‌شود پردازشگر PII ابر عمومی در رابطه با بازیابی، انتقال و یا افشای PII دارای خط‌مشی باشد که در دسترس مشتری خدمات ابری قرار گیرد.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

در برخی نقاط زمانی، ممکن است PII توسط برخی شیوه‌ها نیاز به مرتب‌سازی داشته باشد. این شیوه‌ها ممکن است شامل بازیابی PII مشتری خدمات ابری، انتقال آن به پردازشگر PII ابر عمومی دیگر و یا به یک واپایش‌گر PII (به‌عنوان مثال در نتیجه ادغام)، حذف امن و در غیر این صورت از بین بردن آن، گمنام کردن آن و یا آرشیو آن باشد.

پردازشگر PII ابر عمومی باید اطلاعات لازم را فراهم کند تا به مشتری خدمات ابری اجازه حصول اطمینان از اینکه PII پردازش شده تحت یک قرارداد (توسط پردازشگر PII ابر عمومی و هر یک از پیمانکاران فرعی آن) از هر جایی که برای اهدافی از جمله پشتیبان‌گیری و تداوم کسب‌وکار ذخیره شده و به‌محض آنکه بیشتر از این برای اهداف مشتری لازم نباشند، پاک می‌شود. ماهیت سازوکارهای وضع (حذف لینک، نوشتن، مغناطیس زدایی، تخریب و یا دیگر اشکال پاک کردن) و یا استانداردهای تجاری قابل اجرا باید در قرارداد مشخص شوند.

توصیه می‌شود پردازشگر PII ابر عمومی در رابطه با وضع PII یک خط‌مشی را توسعه داده و اجرا کند و آن را در دسترس مشتری خدمات ابری قرار دهد.

خط‌مشی باید به‌منظور محافظت از مشتری خدمات ابری در مقابل زیان PII به دلیل انقضای تصادفی قرارداد، دوره نگه‌داری PII قبل از تخریب آن پس از اتمام قرارداد را پوشش دهد.

یادآوری- این واپایش و راهنما نیز مربوط به عنصر حفظ اصل «حدود استفاده، حفظ و افشا» است (به الف-۵ مراجعه شود).

الف-۱۰ امنیت اطلاعات

الف-۱۰-۱ توافق‌های محرمانه یا عدم افشا

واپایش

افراد تحت واپایش پردازشگر PII ابر عمومی با دسترسی به PII باید مشمول یک تعهد محرمانه باشند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود یک توافق محرمانه در هر شکل، بین ابر عمومی پردازشگر PII، کارکنان و عوامل آن، نسبت به اینکه کارکنان و عوامل PII را برای مقاصدی جز دستورالعمل‌های مشتری خدمات ابری افشا نمی‌کنند، اطمینان حاصل کند (به الف-۲-۱ مراجعه شود). التزامات توافقنامه محرمانه باید خاتمه هر قرارداد مربوط حفظ کنند.

الف-۱۰-۲ محدودیت ایجاد مواد چاپی

واپایش

ایجاد مواد چاپی نمایش‌دهنده PII باید محدود شود.

راهنمای پیاده‌سازی حفاظت ابر عمومی PII

مواد چاپی شامل مواد ایجاد شده توسط چاپ می‌شود.

الف-۱۰-۳ واپایش و ورود به سامانه بازیابی داده‌ها

واپایش

توصیه می‌شود روش و راه ورودی برای بازیابی داده‌ها وجود داشته باشد.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

یادآوری- واپایش فوق الزامات زیر را که در حوزه‌های خاص به‌کار می‌روند، عمومی می‌سازد. ثبتِ تلاش‌های بازیابی داده‌ها باید شامل موارد: فرد مسئول، شرح داده‌های بازیابی شده و داده‌های بازیابی‌شده به‌صورت دستی باشد.

الف-۱۰-۴ حفاظت از داده‌ها در رسانه ذخیره‌سازی که فرض‌ها را باقی می‌گذارند

واپایش

توصیه می‌شود PII در رسانه‌های که فرض‌های سازمان را باقی می‌گذارند، یک روش‌اجرایی مجوز وجود داشته باشد تا در دسترس کسی غیر از افراد مجاز (مثلاً توسط رمزنگاری داده مربوطه) نباشد.

الف-۱۰-۵ استفاده از رسانه‌ها و افزاره‌های ذخیره‌سازی قابل حمل رمزگذاری نشده

واپایش

رسانه‌های فیزیکی و افزاره‌های قابل حمل که امکان رمزگذاری ندارند به جز در موارد اجتناب ناپذیر نباید استفاده شوند و هرگونه استفاده از این رسانه‌های قابل حمل و افزاره‌ها باید مستند شوند.

الف-۱۰-۶ رمزگذاری PII منتقل شده از طریق شبکه عمومی انتقال داده‌ها

واپایش

توصیه می‌شود PII منتقل شده از طریق شبکه‌های عمومی انتقال داده، قبل از انتقال رمزگذاری شده باشند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

در برخی موارد، به‌عنوان مثال تغییر رایانامه، ویژگی‌های ذاتی سامانه‌های عمومی انتقال داده‌ها ممکن است نیاز داشته باشد که برخی داده‌های ترافیکی در معرض انتقال مؤثر قرار گیرد.

هر جا که ارائه‌دهندگان خدمات چندگانه درگیر ارائه خدماتی از دسته‌های مختلف معماری مرجع رایانش ابری شوند، ممکن است نقش‌های متفاوت یا مشترک در اجرای این راهنما وجود داشته باشد.

الف-۱۰-۷ دسترسی امن به مواد چاپی

واپایش

توصیه می‌شود مواد چاپی در صورت نابودی، به‌صورت امن و با استفاده از سازوکارهایی مانند برش متقاطع، بریدن، سوزاندن، خمیر کردن و غیره امحا شوند.

الف-۱۰-۸ استفاده منحصر به فرد از شناسه‌های کاربر

واپایش

توصیه می‌شود اگر بیش از یک فرد به PII ذخیره‌شده دسترسی داشته باشد، هر یک از آن‌ها به منظور شناسایی، اصالت‌سنجی و مجوز آدرس جداگانه داشته باشند.

الف-۱۰-۹ سوابق کاربران مجاز

واپایش

ثبت به روز از کاربران و مشخصات کاربران با دسترسی مجاز به سامانه اطلاعات باید ایجاد شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

مشخصات کاربر باید برای همه کاربران که دسترسی شان توسط پردازشگر PII ابر عمومی مجاز است، حفظ شود. مشخصات یک کاربر شامل مجموعه‌ای از اطلاعات در مورد آن کاربر، از جمله آدرس کاربر بوده که برای پیاده‌سازی واپایش‌های فنی که دسترسی مجاز به سامانه اطلاعات ارائه می‌کنند، لازم است.

الف-۱۰-۱۰ مدیریت آدرس کاربر

واپایش

شناسه کاربر غیرفعال یا منقضی شده نباید به افراد دیگر واگذار شود.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

در زمینه معماری مرجع رایانش ابری، مشتری خدمات ابری ممکن است مسئول برخی یا تمام جنبه‌های مدیریت آدرس کاربر برای کاربران خدمات ابری تحت واپایش باشد.

الف-۱۰-۱۱ اقدامات قرارداد

واپایش

توصیه می‌شود قرارداد بین مشتری خدمات ابری و پردازشگر PII ابر عمومی، کمینه سنجه‌های فنی و سازمانی برای اطمینان از اینکه ترتیبات امنیتی قرارداد به جا بوده و اینکه اطلاعات را برای اهدافی غیر از دستورالعمل‌های واپایشیِ واپایش‌گر پردازش نمی‌شوند، مشخص کند. توصیه می‌شود چنین سنجه‌هایی در معرض کاهش یک جانبه توسط پردازشگر PII ابر عمومی قرار نگیرند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

التزامات امنیت اطلاعات و حفاظت از PII مربوط به پردازشگر PII ابر عمومی ممکن است مستقیماً از قوانین قابل اجرا ناشی شود. در غیر این صورت التزامات حفاظت PII مربوط به پردازشگر PII ابر عمومی باید تحت پوشش قرار گیرد.

واپایش‌ها در این استاندارد، همراه با واپایش‌های استاندارد ISO/IEC 27002، به‌عنوان کاتالوگ مرجع اقدامات برای کمک به ورود به قرارداد پردازش اطلاعات مربوط به PII در نظر گرفته می‌شوند. توصیه می‌شود پردازشگر PII ابر عمومی قبل از ورود به یک قرارداد مشتری خدمات ابری را از جنبه‌های خدمات حفاظت از PII خود، آگاه سازد.

همچنین توصیه می‌شود پردازشگر PII ابر عمومی در مورد توانایی‌هایش حین فرآیند ورود به قرارداد شفاف باشد. بااین‌حال، درنهایت مسئولیت مشتری خدمات ابری است که از هم‌خوانی اقدامات اجرا شده توسط پردازشگر PII ابر عمومی با التزاماتش اطمینان حاصل کند.

الف-۱۰-۱۲ پردازش PII قرارداد فرعی

واپایش

قراردادهای بین پردازشگر PII ابر عمومی و هرگونه پیمانکار فرعی برای پردازش PII، باید کمینه اقدامات فنی و سازمانی که با امنیت اطلاعات و التزامات حفاظت از پردازشگر PII ابر عمومی هماهنگ است را مشخص کند. چنین اقداماتی نباید در معرض کاهش یک‌جانبه توسط پیمانکار فرعی[1] قرار بگیرد.

1 - Sub-contractor

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

استفاده از پیمانکار فرعی برای ذخیره نسخه پشتیبان توسط این واپایش (به الف-۷-۱ مراجعه شود) پوشش داده می‌شود.

الف-۱۰-۱۳ دسترسی به داده‌ها از فضای ذخیره‌سازی از قبل استفاده شده

واپایش

توصیه می‌شود پردازشگر PII ابر عمومی مطمئن شود که پس از اختصاص فضای ذخیره‌سازی داده‌ها به یک مشتری خدمات ابری، هرگونه اطلاعاتی که قبلاً در آن فضای ذخیره‌سازی وجود داشته، برای مشتری قابل رؤیت نیست.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

از طریق حذف داده‌های یک سامانه اطلاعات توسط یک کاربر خدمات ابری، مسائل مربوط به عملکرد ممکن است به معنی غیرعملی بودن پاک شدن صریح و روشن آن داده‌ها باشد. این امر ممکن است خطر خوانده شدن داده‌ها توسط کاربر دیگر را ایجاد کند. از چنین خطری باید با اقدامات فنی خاص اجتناب شود.

هیچ راهنمای خاصی برای اجرای تمام موارد این واپایش به طور ویژه مناسب نیست. بااین‌حال، به‌عنوان یک مثال، برخی از زیرساخت‌های ابری، سیستم‌عامل و یا برنامه‌های کاربردی، درصورتی‌که یک کاربر خدمات ابری برای خواندن فضای ذخیره‌سازی که توسط داده‌های وی دوباره نوشته نشده تلاش کند، به صفر بازگشت می‌کنند.

الف-۱۱ انطباق حریم خصوصی

الف-۱۱-۱ موقعیت جغرافیایی PII

واپایش

توصیه می‌شود پردازشگر PII ابر عمومی کشورهایی که PII احتمالا ممکن است در آن‌ها ذخیره شود را مشخص و مستند کند.

راهنمای پیاده‌سازی حفاظت از PII در ابر عمومی

توصیه می‌شود هویت کشورهایی که PII احتمالا در آن‌ها ذخیره می‌شود، در دسترس مشتریان خدمات ابری قرار گیرد. هویت این کشورها با استفاده از پردازش تحت قرارداد PII باید در نظر گرفته شود. هر جا توافقات قراردادی خاص برای انتقال بین‌المللی داده‌ها اعمال شود، مانند الگوی بندهای قرارداد، قوانین شرکت‌های بزرگ و یا قوانین عبور از مرز حفظ حریم خصوصی، توافق‌نامه‌ها، کشورها و یا شرایطی که چنین توافقی تحت آن‌ها اعمال می‌شود نیز باید مشخص شود. توصیه می‌شود پردازشگر PII ابر عمومی به موقع مشتری خدمات ابری را از هرگونه تغییر در نظر گرفته شده در این زمینه آگاه سازد طوری که مشتری خدمات ابری امکان اعتراض به این تغییرات و یا فسخ قرارداد را داشته باشد.

الف-۱۱-۲ مقصد مورد نظر PII

واپایش

توصیه می‌شود PII منتقل شده با استفاده از شبکه انتقال داده‌ها در معرض واپایش‌های مناسب طراحی شده به منظور اطمینان از رسیدن داده‌ها به مقصد مورد نظر قرار گیرد.

کتاب‌نامه

[1] BS 10012:2009, Data protection. Specification for a personal information management system

[2] ENISA. Report on Cloud Computing: Benefits, risks and recommendations for information security, November 2009 (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport)

[3] European Union, Article 29 Working Party, Opinion 05/2012 on Cloud Computing, adopted July 2012: (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf)

[4] ISO/IEC 17789, Information technology — Cloud computing — Reference Architecture

[۵] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

[۶] استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

[7] ISO/IEC 27036-4, Information technology — Information security for supplier relationships — Part 4: Guidelines for security of Cloud services

[8] ISO/IEC 27040, Information technology — Security techniques — Storage security

[9] ISO/IEC 29101, Information technology — Security techniques — Privacy architecture framework

[10] ISO/IEC 29134, Information technology — Security techniques — Privacy impact assessment —Methodology

[11] ISO/IEC 29191, Information technology — Security techniques — Requirements for partiallyanonymous, partially unlinkable authentication..

[12] ISO/IEC JTC 1/SC 27, WG 5 Standing Document 2 — Part 1: Privacy References List. Latest version available at: http://www.jtc1sc27.din.de/sbe/wg5sd2

[13] JIS Q 15001:2006, Personal information protection management systems — Requirements

[14] NIST SP 800-53 rev4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

[15] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),April 2010 (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf)

[16] NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011(http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf)