Data Protection is ***People*** *Protection*

إرشادات حماية البيانات والخصوصية

MERCY CORPS

صُمم المُحتوى التالي خصيصًا لمساعدة فريق ميرسي كور على فَهْم الاستخدام المسؤول للبيانات وتطبيق ممارسات استخدام البيانات المسؤولة. فهو يجمع بين العديد من سياسات ميرسي كور الحالية، ووثائق الإرشادات مع بعض البرامج التعليمية البسيطة وروابط لمصادر أخرى. يمكن استخدام المعلومات معًا كدليل إرشادي شامل، أو استخدام كل قسم كدليل مستقل لموضوع بعينه.

وفي حين أن الدليل مُصمم خِصيصًا لموظفي ميرسي كور، ومواكبة مجموعة أدوات البيانات المسؤولة ، إلا أننا نصدره بترخيص مفتوح حتى يعود بالفائدة على شُركائنا، ونُظرائنا من المُنظمات، وغيرهم ممن يحتاجون إلى أمثلة لسياسات وقوالب وتعليمات لتنفيذ ممارسات الاستخدام المسؤول للبيانات. يمكنك تنزيل كل محتوى الدليل الخاص بنا عبر صفحتنا علىGithub . https://github.com/mercycorps/DPP-guides

جدول المحتويات

الاقتباسات والشكر والتقدير

يعد المحتوى المقدم في هذا الدليل جزءًا من ممارسات الإدارة المُثلى للبيانات، ودورة أكبر لحياة البيانات، أو الأنشطة العامة لإدارة البيانات الفردية كجزء من برنامج أو تلبية. تعد الموارد التالية مواقع ممتازة للبدء منها في فهم أكثر نُضجًا لإدارة بياناتك بمسؤولية. لقد استخدمنا أو اقتبسنا أجزاء من جميع هذه الموارد في الدليل بأكمله، ونشير إلى فصول أو أقسام محددة أكثر صلة بموضوع معين.

- إن مجموعة أدوات شراكة التعلم النقدي لمسؤولية البياناتمُصممة على وجه التحديد لمُستخدمي النقد والقسائم، ولكنها معيار ذهبي في توجيه البيانات المسؤولة. مجموعة الأدوات متاحة بالإنجليزية و العربية و الفرنسية ، و الأسبانية.
- تُتيح شبكة عمل تعلم التحويل النقدي الإلكتروني مجموعة أدوات بدء البيانات للموظفين الميدانيين في المجال الإنساني يوفر سلسلة من أوراق النصائح الخاصة بالبيانات لفهم الجوانب المختلفة لإدارة البيانات الجيدة وممارسات الحماية..
- دليل اللجنة الدولية للصليب الأحمر لحماية البيانات في العمل الإنساني وهو دليل مفصل لكل جانب من جوانب البيانات الإنسانية تقريبًا.
- دليل بيانات الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر هي مورد ممتاز للتمارين وخطط الجلسات وقوائم المراجعة والمواد الأخرى لمساعدتك على تنظيم المحادثات والأنشطة مع فريقك لتطوير أنشطة البيانات المسؤولة.
- البرنامج التعليمي عبر الإنترنت لمركز البيانات الإنسانية لعمل تقييم لمخاطر الإفصاح هو مورد تقني محدد للغاية، ولكنه مورد لا غنى عنه لتقليل مخاطر استخدام البيانات لتعريف الأفراد.
- دليلEngine Room لاختصاصي التنمية الحديثة نظرة عامة جيدة للبيانات في سياق أنشطة التنمية الدولية.

الترخيص

فهم البيانات الحساسة

قد يكون فهم التصنيفات المختلفة للبيانات أمرًا صعبًا، لكنه جزء مهم من العمل مع البيانات الإنسانية. فمثلًا، ما الفرق بين البيانات الشخصية والبيانات الحساسة؟ قد تحتاج أنواع معينة من البيانات عناية خاصة وفقًا للقوانين الإقليمية أو الوطنية أو السياسات التنظيمية، ويمكن أن تمثل مخاطر مُختلفة لكل من المشاركين في البرنامج والمنظمات. فالبيانات الحساسة هي فئة فرعية من البيانات الشخصية ويقدم هذا القسم إرشادات مفصلة لمعالجتها وفهمها.

☆ الأهمية

تجمع غالبية برامج ميرسي كور والأنشطة الأخرى نوعًا من البيانات الشخصية عن الأفراد. وفي كثير من الحالات، تقوم البرامج أيضًا بجمع معلومات حول الملف الشخصي الثقافي للفرد، أو الميول الجنسية، أو الصحة أو القياسات الحيوية والجينات. وتعتبر هذه الأنواع من المعلومات بيانات حساسة، وإذا تم الإفصاح عنها أو الوصول إليها أو مشاركتها بشكل غير صحيح، فقد يؤدي ذلك إلى:

- إلحاق الضرر بشخص ما، مثل العقوبات والتمييز والتهديدات الأمنية؛
- تأثير سلبي على قدرة ميرسي كور على تنفيذ الأنشطة وتقليل الثقة أو الإدراك العام.

فمن الضروري اتخاذ الخطوات اللازمة لحماية هذه البيانات.

الإرشاد

يحتوي هذا القسم على وثيقتين:

- "إرشادات معالجة البيانات الحساسة" والتي تُعرفك بالبيانات الحساسة، والمصطلحات الأساسية، والأشياء التي يجب مراعاتها عند التخطيط لجمعها وتخزينها وتحليلها ومشاركتها.
  - يمكن لموظفي ميرسي كور الوصول إلى هذه الإرشاداتفي المكتبة الرقمية الداخلية لمُنظمة ميرسي كور.
  - كما يمكن لأي شخص تنزيل مستند الإرشادات باللغات الإنجليزي و العربية و الأسبانية و الفرنسية ، و الروسية.
- يمكن استخدام "نموذج تقييم المعلومات الحساسة (SIA)" مع تقييم تأثير الخصوصية لتوثيق جميع الضمانات الإضافية المستخدمة للبيانات الحساسة. تحدد هذه الوثيقة أيضًا الأسس القانونية المختلفة التي يمكن استخدامها لتبرير جمع واستخدام البيانات الحساسة.
  - يمكن لموظفي ميرسي كور الوصول إلى نموذج SIA في المكتبة الرقمية الداخلية لمُنظمة ميرسي كور.
  - يمكن لأي شخص تنزيل القالب كمستند بتنسيق "وورد" باللغات إنجليزي و العربية و الأسبانية و الفرنسية ، و الروسية.

مساعدة إضافية

يجب أن يكون التخطيط لجمع البيانات الحساسة أو استخدامها جزءًا لا يتجزأ من استراتيجية أكبر لدورة حياة البيانات لبرنامج أو نشاط ما. توجد العديد من الموارد التي من شأنها مُساعدتك في هذا الصدد.

- دليل بيانات الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر *(IFRC)*وهو مورد ممتاز للتمارين، وخطط الجلسات، وقوائم المراجعة، وغيرها من المواد الأخرى التي تُساعدك على تنظيم المحادثات والأنشطة مع فريقك لتطوير أنشطة البيانات المسؤولة. وعلى وجه الخصوص، الوحدة 4- البيانات المسؤولة هي اَلْوَحْدَة المُثلى للبدء منها.
- دليل اللجنة الدولية للصليب الأحمر لحماية البيانات في العمل الإنساني وهو دليل مفصل لكل جانب من جوانب البيانات الإنسانية تقريبًا. حيث يتناول الفصل 3 تحديدًا الأساس القانوني لمعالجة البيانات الشخصية.
- إن مجموعة أدوات شراكة التعلم النقدي لمسؤولية البياناتمُصممة على وجه التحديد لمُستخدمي النقد والقسائم، ولكنها معيار ذهبي في توجيه البيانات المسؤولة. تحديدًا، ورقة النصائح # *2* ، "التصميم والتخطيط" التي تُناقش الأساس القانوني للبيانات الحساسة. مجموعة الأدوات متاحة بالإنجليزية و العربية و الفرنسية ، و الأسبانية.

تقييمات تأثير الخصوصية

يساعدك هذا الدليل على فهم تقييم تأثير الخصوصية (PIA)، فهو يحتوي على إرشادات تقييم تأثير الخصوصية، والنموذج المستخدم في ميرسي كور. يحتوي نموذج تقييم تأثير الخصوصية على سلسلة من الأسئلة التي تنشئ إطارًا لتعريف مخاطر الخصوصية المحتملةذات الصِلة بجمع البيانات وإدارتها، والتي تعد جزءًا من تنفيذ برنامج أو تقنية جديدة. يعتبر تقييم تأثير الخصوصية (PIA) مهمًا أيضًا عندما يتغير سياق البرنامج بشكل كبير، فيجب النظر إلى المخاطر أو السيناريوهات الجديدة بعين الاعتبار.

إن تقييم تأثير الخصوصية مطلوب في أي وقت لبرنامج أو مشروع أو تقنية جديدة تنطوي على جمع أو استخدام بيانات شخصية أو حساسة.

☆ الأهمية

يُتيح لك تقييم تأثير الخصوصية (PIA) تحليل كيفية تأثير مشروع معين أو تقنية جديدة على خصوصية الأفراد المعنيين. كما يساعد تقييم تأثير الخصوصية (PIA) أيضًا على توثيق استراتيجيات التخفيف التي من شأنها حماية خصوصية المشاركين وتعزز ثقة الجمهور في عملنا. يضمن تقييم تأثير الخصوصية (PIA) التحديد المُبكر للمشكلات المحتملة، حيث تكون معالجتها أبسط وأقل تكلفة، ولن تكون هُناك مُخاطرة بإيذاء المشاركين في البرنامج أو الموظفين.

المبادئ

المبادئ الكامنة وراء تقييم تأثير الخصوصية (PIA) هي على غِرار تلك الخاصة بأي استخدام آمن للبيانات الشخصية. فيما يلي بعض المبادئ الأساسية التي تم تكييفها من The Cash Learning Partnership (CaLP) :

- تحديد مخاطر الخصوصية للأفراد.
- تحديد مسئوليات حماية البيانات والخصوصية لمنظمتك.
- إظهار المساءلة والامتثال للسياسات التي تحمي المشاركين والشركاء والموظفين في البرنامج.
- التأكد من أن المنظمة تعزز الحق في الخصوصية في أنشطتها الإنسانية وتعمل كمسؤول أخلاقي للبيانات.

الإرشاد

يمكن لموظفي ميرسي كور العثور على إرشادات PIA في المكتبة الرقمية. تحتوي الوثيقة على إجابات للأسئلة المتداولة ذات الصلة بـ بتقييمات تأثير الخصوصية، وروابط لأرشيف ميرسي كور الداخلي لتقييمات تأثير الخصوصية المكتملة للمقارنة. دليل تقييم تأثير الخصوصية الخاص بميرسي كور مُتاح لأي شخص باللغات التالية:الإنجليزي و العربية و الأسبانية و الفرنسية ، و الروسية.

تذكر أن:

- تقييم تأثير الخصوصية هو معالجة تُستخدم لتحديد وتقليل مخاطر الخصوصية. إكمال نموذج تقييم تأثير الخصوصية ليس نهاية المطاف! أعد زيارة تقييم تأثير الخصوصية (PIA) مرة أخرى بعدما يبدأ مشروعك للتأكد من عدم وجود تغييرات جديدة تؤدي إلى مخاطر جديدة. وإذا كان هناك أي مخاطر جديدة، فم بعمل التغييرات واستراتيجيات التخفيف الجديدة اللازمة لتقليل أي مخاطر جديدة.

- يتضمن إجراء تقييم تأثير الخصوصية (PIA)العمل مع الأشخاص في ميرسي كور ، وأحيانًا مع المنظمات الشريكة وغيرها لتحديد مخاطر الخصوصية وتقليلها. على سبيل المثال ، إذا كنت تستخدم تقنية جديدة ، فقد تحتاج إلى البحث عما إذا كانت الشركة التي تعمل معها لديها سياسة خصوصية، وما هي الضمانات التكنولوجية التي تستخدمها لضمان حماية البيانات. قد تحتاج أيضًا إلى تثقيف نفسك بشأن لوائح الخصوصية ذات الصلة في البلد الذي تعمل فيه. إليك ثلاثة مواقع إلكترونية يمكنك استخدامها لمراقبة البيانات على المستوى ادولي وقوانين الخصوصية هي:
  - قوانين حماية البيانات في العالم؛
  - وهوقاعدة بيانات مؤتمر الأمم المتحدة للتجارة والتنمية الخاصة بتشريعات حماية البيانات والخصوصية في جميع أنحاء العالم ؛ و
  - قاعدة البيانات الارشاداد الموحدة لقوانين الخصوصية العالمية.
- قد يكون من المفيد مقارنة تقييمات تأثير الخصوصية لبرامج مماثلة. ويمكنك إجراء هذا البحث بنفسك، أو التواصل مع فريق حماية البيانات والخصوصية للحصول على المساعدة.

النماذج

يمكن لموظفي ميرسي كور العثور على النموذج المُطوللتقييم تأثير الخصوصية في المكتبة الرقمية. كما أن نموذج تقييم تأثير الخصوصية المُطوّل متاح لأي شخص باللغات التالية:الإنجليزي و العربية و الأسبانية و الفرنسية ، و الروسية.

ويتضمن كل نموذج مُطوّل من نماذج تقييم تأثير الخصوصية خمس حالات استخدام ، موضحة أدناه. ينقلك النقر فوق الروابط أدناه إلى شاشة يمكن لأي شخص منها تنزيل الإصدارات الإنجليزية من حالات الاستخدام الفردية بتنسيق**.odt** (متوافق مع مايكروسوفت وورد، والتطبيقات مفتوحة المصدر مثل OpenOffice و LibreOffice) وذلك من خلال النقر فوق زر **مشاهدة** أو **تحميل**.

- سياسة جديدة
- إجراء أو عمليةجديدة
- برنامج أو نظام تكنولوجيجديد
  - وهذا في المقام الأول لتنفيذ أنظمة عالمية جديدة ،أو على مستوى الدولة أو فريق معين.
  - إذا كنت تختار نظامًا جديدًا، أو تستخدمه كجزء من مشروع أو برنامج أكبر ، فاستخدم خيار المشروع أو البرنامج بدلاً من ذلك.
- مُتعهد أو شريكجديد
  - يهدف هذا في المقام الأول إلى التحقق من صحة أنشطة البائع أو الشريك أو الطرف الثالث كجزء من نشاط فريد أو نشاط لمرة واحدة.
  - إذا كنت تختار مورّدًا جديدًا أو شريكًا أو طرفًا ثالثًا أو تستخدمه كجزء من مشروع أو برنامج أكبر ، فاستخدم خيار المشروع أو البرنامج بدلاً من ذلك.
- مشروع أو برنامججديد
  - يمكن أن يكون هذا لأي مرحلة أو جانب من جوانب المشروع أو البرنامج.
  - هذا هو خيار تقييم تأثير الخصوصية الأكثر شمولاً ، ويتضمن لغة لاختيار برامج أو أنظمة تقنية جديدة و / أو بائع أو شريك جديد.

مساعدة إضافية

- توفر مجموعة بدء المعلومات لشبكة عمل تعلم التحويل النقدي الإلكتروني ورقة نصائح خاصة بالبيانات لتقييمات تأثير الخصوصية (PIAs) **(أنظر صفحة النصائح # 1)**
- يُتيح مكتب مفوضية المعلومات في المملكة المتحدة أ مدونة تفصيلية لممارسة لإجراء تقييمات تأثير الخصوصية .
- دليل اللجنة الدولية للصليب الأحمر لحماية البيانات في العمل الإنساني وهو دليل مفصل لكل جانب من جوانب البيانات الإنسانية تقريبًا. يتناول الفصل 5 تحديدًا تقييمات تأثير الخصوصية.

أفضل الممارسات في مشاركة الملفات

يغطي هذا الدليل أفضل ممارسات مشاركة الملفات لأعضاء فريق ميرسي كور باستخدام تطبيقات G Suite، وخاصة Google My Drive. لتبسيط هذا الدليل، سنناقش مشاركة *ملف واحد*، كجدول بيانات. ومع ذلك، تتوفر نفس الخيارات عند مشاركة *مُجلدات* My Drive.

ملاحظة: تنتقل ميرسي كور إلى Microsoft 365 لمشاركة الملفات. **بمجرد إنشاء أفضل الممارسات لهذه المِنصة، سيتم إنشاء مستند أو مورد مماثل.**

☆ الأهمية

هناك عِدة أسباب تجعل من الأفضل مشاركة ملف عن طريق الاستضافة على جوجلDrive، وإرسال رابط بدلاً من إرسال الملف كمرفق في رسالة البريد الإلكتروني.

- الأمان: يمكنك بسهولة تغيير الأشخاص المسموح لهم بالوصول إلى ملفك أو التعديل عليه. يمكنك أيضًا تجعل الرابط مُحدد بوقت، وذلك من خلال السماح فقط بالوصول إلى الملف خلال فترة زمنية معينة.
- التحكم في الإصدار: عند مشاركة ملف مستضاف عبر الإنترنت ، يمكن للعديد من الأشخاص الوصول إليه مرة واحدة، وتظل جميع التغييرات والتعليقات في ملف واحد. غالبًا ما ينتج عن إرسال ملف كمرفق إصدارات متعددة من نفس المستند وبأسماء ملفات وتعديلات وتعليقات مختلفة وما إلى ذلك. وسيقضي مالك المستند وقتًا طويلاً في محاولة تجميع كل هذا في ملف واحد! أما عند استخدام الرابط فيتمتع المُستلمين بإمكانية الوصول إلى الإصدار الأحدث من المُستند.
- أحجام الملفات: تفرض بعض أقسام تقنية المعلومات قيودًا على حجم المرفقات المسموح بها. أما إرسال رابط فيُتيح لك مشاركة الملفات باختلاف أحجامها.
- سهولة التحرير: الملفات التي تتم مشاركتها كمستندات على Drive أو Microsoft Word أو OneDrive أو ما شابه من التنسيقات، تُتيح للمستلم فتح المستند والتفاعل معه باستخدام مُتصفح الويب: ولا يلزم أن يكون لديهم أحدث إصدار من نوع معين من البرامج.

المبادئ

يجب مراعاة ما يلي عند مُشاركة المستندات:

- **ضع في اعتبارك مَن سيقوم بإنشاء الملف أو المجلد ، ومن سيمتلكه / يديره ، ومن سيصل إليه. إذا قام المُتعهد على المدى القصير بإنشاء الملفات وإدارتها ، فهناك خطر من أن الملفات أو أن الوصول إليها يترك للمُتعهدين عند مغادرتهم!**
  - امنح حق الوصول فقط لأولئك الذين يحتاجون إلى الملف.
  - يجب أن يكون هُناك قيود على الوصول إلى محتوى المعلومات السرية، أو الخاصة، أو معلومات التعريف الشخصية (PII) دائماً. إذا كنت غير قادر على تحديد ما إذا كان يجب وضع قيود على المحتوى، أو كيفية وضع تلك القيود، فالرجاء طلب المساعدة من الشؤون القانونية أو فريق حماية البيانات والخصوصية.

❯ استخدم المستوى المناسب من الأذونات.

- ضع في اعتبارك مثالاً حيث يلزم إنشاء اتفاقية مشروع جديد. وعلى الأرجح ، ينبغي أن يتمتع الفريق المسؤول عن إنشاء الاتفاقية فقط بالوصول الكامل. وعندما يحين وقت استلام التعليقات من الآخرين ، امنح أذونات إضافية تسمح لهم فقط بالمشاهدة أو التعليق.
- توخ الحذر الشديد عند منح أذون الوصول لأعضاء الفريق الذين قد يستخدمون حسابات البريد الإلكتروني الشخصية الخاصة بهم عن طريق الخطأ. فبدلاً من منحهم الوصول بواسطة حساب بريد إلكتروني شخصي ، امنحهم حق الوصول بواسطة حسابهم في ميرسي كور ، واطلب من عضو الفريق تسجيل الدخول باستخدام بيانات الاعتماد هذه.

❯ تتغير الأذونات بمرور الوقت

- إذا كنت تعمل فقط مع شخص ما لفترة قصيرة من الوقت أو مع أشخاص خارج ميرسي كور ، فضع في اعتبارك منح أذونات مؤقتة. وإذا نسيت إزالة حق الوصول لاحقًا ، فسيعمل تاريخ انتهاء الصلاحية على تعليق وصولهم في الوقت المناسب.
- دقق قائمة الأشخاص المُخول لهم الوصول إلى ملفاتك أو مجلداتك أو محركات الأقراص المشتركة بشكل دوري للتأكد من الغاء حق الوصول لأعضاء الفريق الذين تغيرت وظائفهم أو لم يعودوا يعملون مع ميرسي كور.

❯ يتطلب المحتوى المحفوف بالمخاطر خطوات إضافية

- إن معلومات التعريف الشخصية (PII) أو معلومات التعريف الديموغرافية (DII) أو أنواع أخرى من البيانات الشخصية محمية بموجب قوانين حماية البيانات المتعددة. فقبل مشاركة البيانات الشخصية، تحقق من المتطلبات القانونية لمشاركة هذه المعلومات مع الآخرين. يمكن أن تؤدي مشاركة البيانات الشخصية غير الملائمة إلى تعرُّض المشاركين في البرنامج، والمُتبرعين، والشركاء وأعضاء فريق ميرسي كور للخطر. إذا كانت لديك أسئلة حول البيانات الشخصية، أو قوانين حماية البيانات ، يرجى إرسال بريد إلكتروني إلى فريق حماية البيانات والخصوصية على dataprotection@mercycorps.org.
- إذا أعتُبِرت المعلومات سرية أو مملوكة لأغراض تجارية، شاركها فقط مع الأطراف المعنيَّة وضع في اعتبارك منح أذونات الوصول المؤقتة.
- إذا أعتُبِرت المعلومات سرية أو مملوكة لأغراض تجارية، شاركها فقط مع الأطراف المعنيَّة وضع في اعتبارك منح أذونات الوصول المؤقتة. راجع قسمي التشفير وإلغاء تحديد الهوية لمزيد من الأمثلة حول كيفية القيام بذلك.

❯ لا تنقل الملفات مُطلقًا دون إذن من مالكه.

- قد يغير نقل الملفات الأشخاص المُخوَّل لهم الوصول إليها، مما يجعل من المستحيل على الآخرين العثور على الملف! فتحقق دائمًا من مالك المستند قبل نقل ملف تمت مُشاركته إلى موقع جديد.

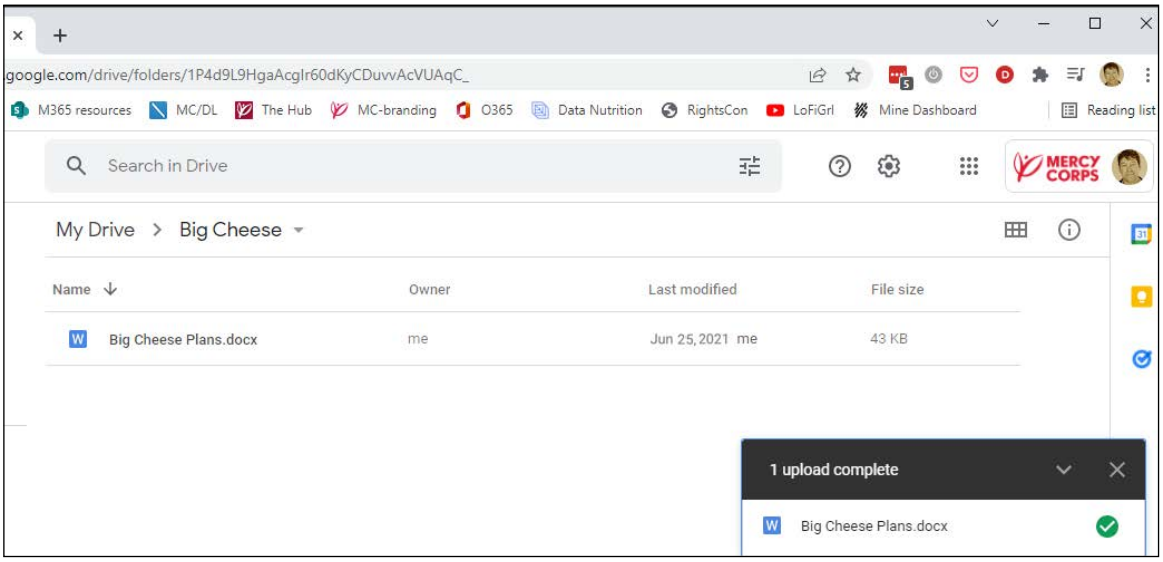
مشاركة الملفات:GDrive

فيما يلي نموذج لاستخدام مشاركة ملف بأفضل الممارسات في Google Drive. تخيل أننا العام الحالي هو 2020 ،وأن ميرسي كور تعمل مع مستشار (PNW Rocks) لإنشاء مواد لمبادرة كبيرة جديدة في ميرسي كور ، والتي تحمل الاسم الرمزي"Big "Cheese. ولن يُعلن عن مشروع "Big Cheese" حتى يوليو 2021 ، لذا من المهم تحديد مَن يمكنه الوصول إلى الملف. للبدء، نُريد التعاون بشأن الخطوات التالية للمشروع من خلال ملف يسمى "Big Cheese Plans".

التعليمات

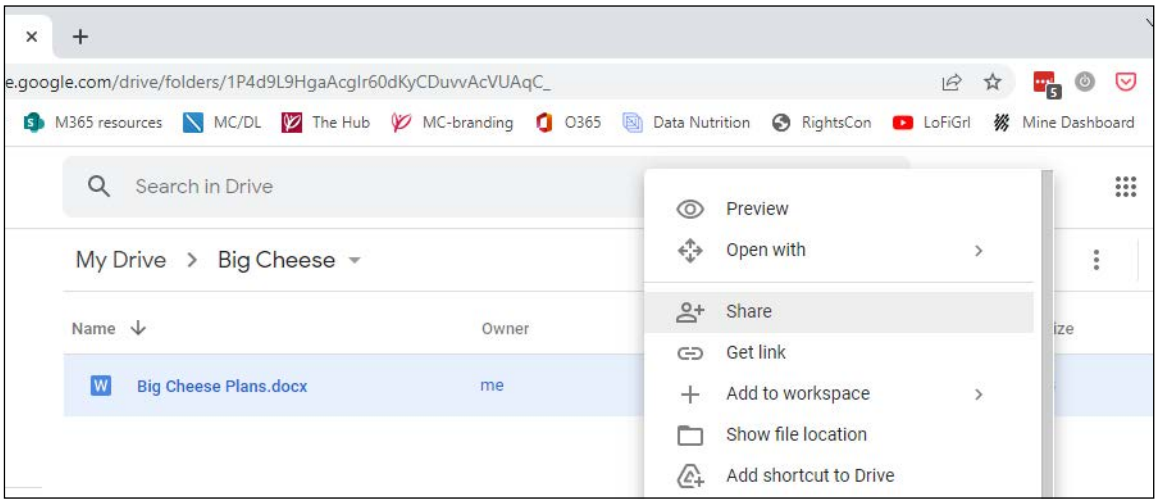
الخطوة 1 - رفع الملف

ارفع الملف إلى My Drive.



الخطوة 2 - مُشاركة الملف

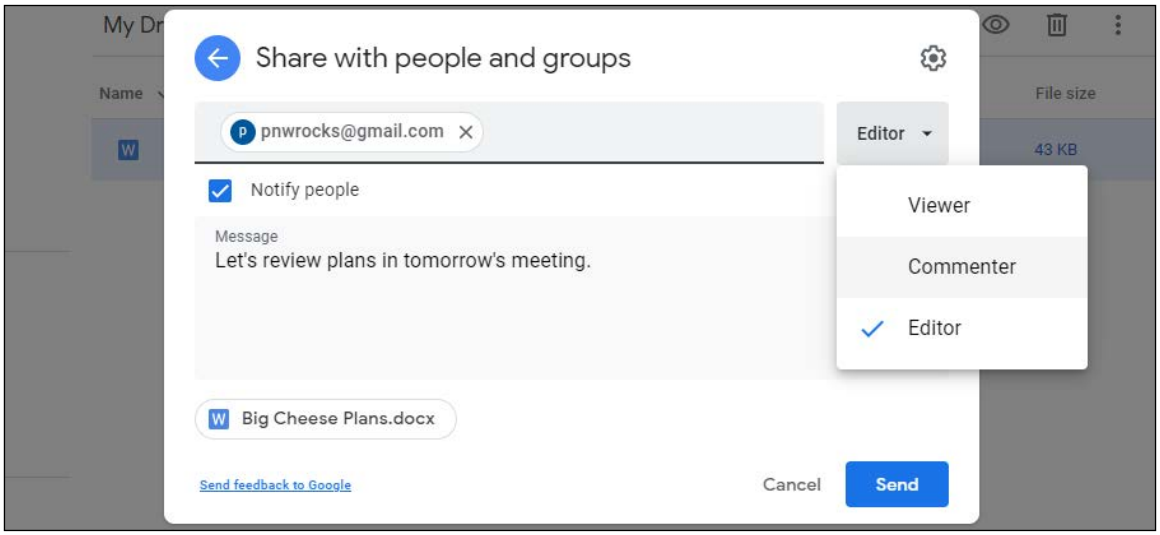
لمشاركة الملف ، انقر بزر الماوس الأيمن فوق الملف ثم انقر فوق **مُشاركة**.



- امنح حق الوصول فقط لأولئك الذين يحتاجون إلى الملف. عند مشاركة ملف في My Drive ، يكون الإعداد الافتراضي هو **مُقيَّد** (مُقيد للأشخاص أو المجموعات) ، وهي أفضل ممارسة. تذكر، أنه يجب أن يكون هُناك قيود على الوصول إلى محتوى المعلومات السرية، أو الخاصة، أو معلومات التعريف الشخصية (PII) دائماً.
- يجب استخدام خيار **أي مُستخدم لديه الرابط**فقط للملفات التي لا تحتوي على معلومات سرية وتكون مفتوحة للجمهور. أما استخدام **أي مُستخدم لديه الرابط**لملف يحتوي على بيانات سرية خاصة، أو شخصية، أو مالية ، فمن المُمكن مشاركته بسهولة، أو عن غير قصد وهذا يُعرِّض ميرسي كور لمخاطر قانونية فورية، ويُسهّل استخدام الجهات السيئة للمعلومات في أغراض إجرامية.

الخطوة 3 - تحديد مستوى الوصول

أدخل عنوان البريد الإلكتروني للشخص الذي تريد مشاركة الملف معه ، ثم اختر مستوى الوصول. الوضع الافتراضي لوصول في جوجل هو **مُحرر**، وهو مُلائم فقط لأعضاء الفريق الذين يحتاجون إلى الوصول الكامل إلى المستند. أما عندما تقوم بإشراك المالكين للحصول على آرائهم ، اختر **عارض** أو **مُعلِّق**. أفضل الممارسات هي إخطار الشخص وإضافة رسالة توضح سبب مشاركة الملف. للإشعار، اترك علامة**إشعار الأشخاص** كما هي. عندما تنتهي من التغييرات، انقر فوق **ارسال**.

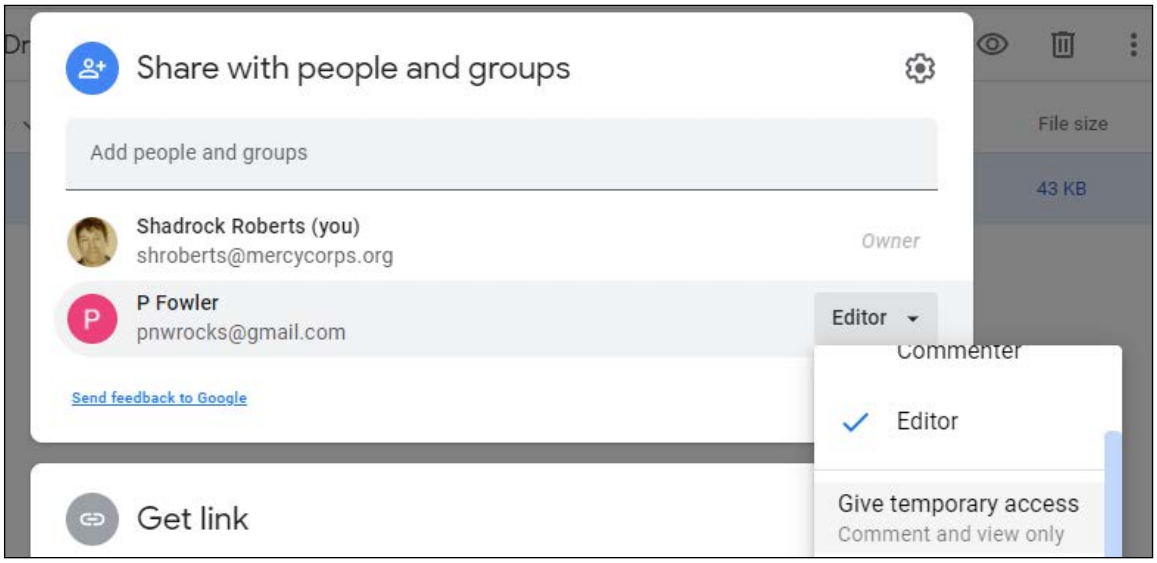


خيار آخر هو إرسال بريد إلكتروني منفصل يحتوي على رابط للملف. للإشعار بشكل منفصل عبر البريد الإلكتروني ، أزل العلامة من مربع الاختيار**إشعار الأشخاص** . بعد النقر **تم** ، انقر بزر الماوس الأيمن فوق الملف واختر **الحصول على الرابط** . في النافذة المنبثقة الجديدة ، انقر فوق زر**نسخ الرابط**، ثم الصقه في بريدك الإلكتروني.

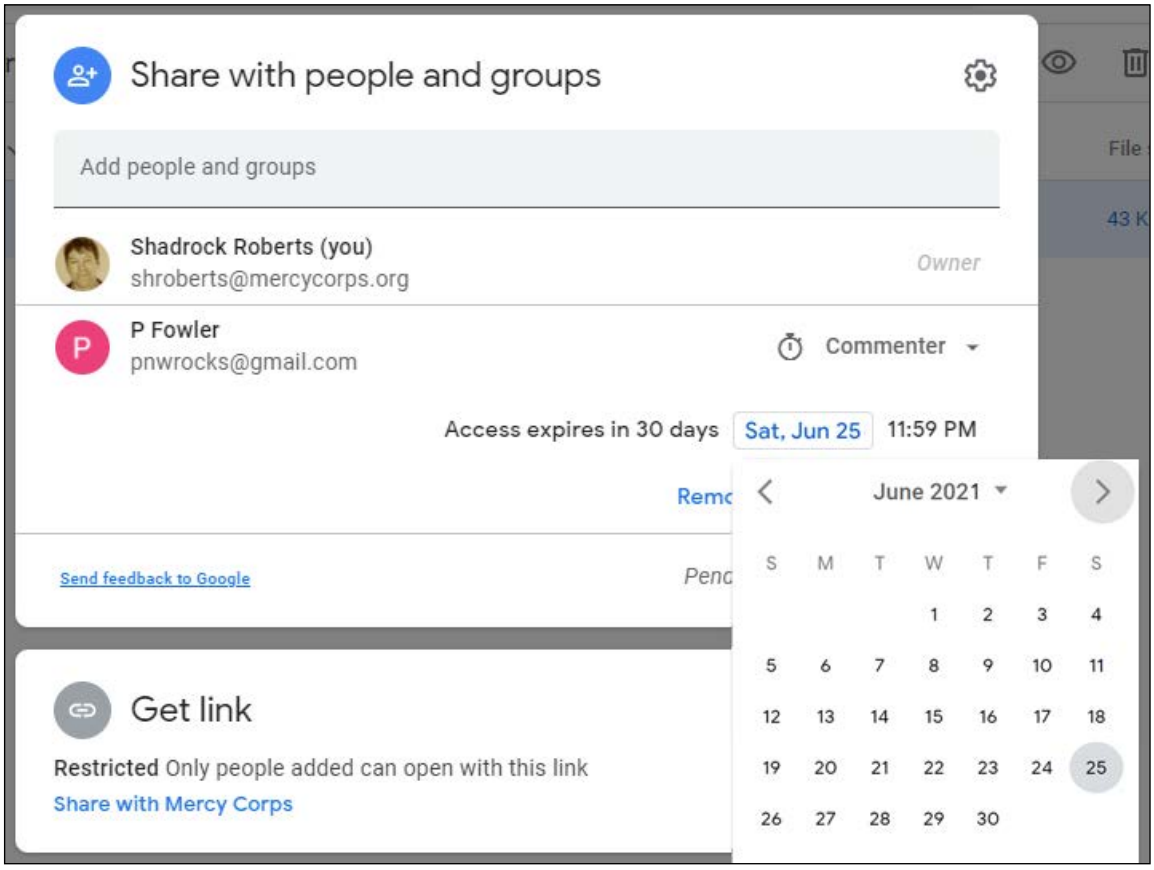
- لمعرفة المزيد حول مستويات الوصول ، تفضّل بزيارة شارك وتعاون في My Drive.
- إذاقيدَّت ملف ، وقام شخص ما لديه حق الوصول بمشاركة الرابط مع شخص آخر ، فلن يتمكن هذا الشخص تلقائيًا من الوصول إلى هذا المحتوى في Google Drive. بل يرى صفحة ويب بها امكانية طلب حق الوصول. وسيُرسل طلب حق الوصول إلى مالك الملف. ينبغي مراجعة طلبات الوصول ، ولا ينبغي لمن يتلقون طلبات الوصول منح الإذنللطلبات أو أي منها، دون مراجعة الملاحظات والاعتبارات المذكورة أعلاه.

الخطوة 4 - الوصول المؤقت

بمجرد منح الإذن ، يمكن تخفيض الفترة الزمنية للمشاركة. ولتقييد الوصول انقر بزر الماوس الأيمن فوق الملف مرة أخرى ، ثم انقر فوق **مُشاركة**. ابحث عن عنوان البريد الإلكتروني الذي شاركته للتو وانقر بزر الماوس الأيمن فوق مستوى الوصول. سترى خيارات جديدة تظهر ؛ حدد**منح حق وصول مؤقت**.



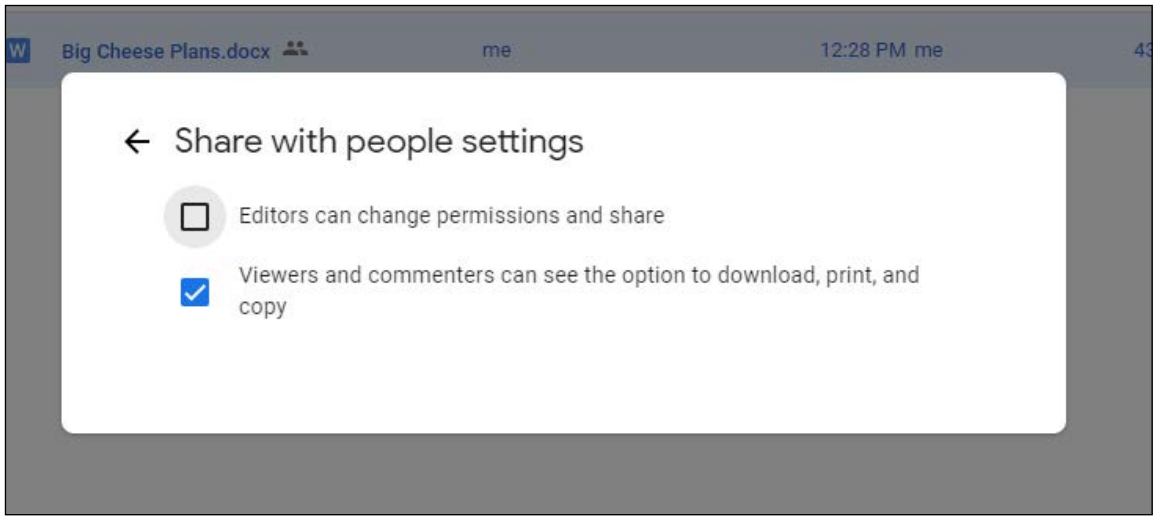
سيظهر لك التقويم. انتقل إلى الشهر الذي تُريد أن تنتهي فيه صلاحية الوصول ، وانقر فوق التاريخ المقابل.



سيختفي التقويم ، ويتغير تاريخ العرض. وعندما ترى أن الوصول سوف تنتهي صلاحيته في التاريخ الصحيح، انقر **حفظ**.

الخطوة 5 - خيارات إضافية

إذا كانت لديك مخاوف بشأن قيام الآخرين بإجراءات غير مناسبة مع المحتوى، توجد خيارات إضافية متاحة في شاشة الإعدادات. حيث يمكن الوصول إلى إعدادات الملف من خلال رمز الترس أعلى يمين نافذة المشاركة. انقر فوق الترس وستظهر لك خيارات المزيد من قيود المشاركة، أو تعطيل خيار التنزيل أو الطباعة أو النسخ. بالنسبة لأي خاصيَّة تريد تعطيلها ، ما عليك سوى إزالة العلامة من مُربع التحديد. وسيتم تحديث الملف، وحفظ الإعداد الجديد بسرعة.



❱ لمعرفة المزيد ، تفضَّل بزيارة خيارات تقييد المشاركة في Drive.

اعتبارات إضافية

- لا تضع ملفات سرية داخل مجلدات يتم مشاركتها على نطاق واسع. تُمنح أذونات المجلدات المشتركة لكل ملف ومجلد فرعي ، لذلك يمكن لأي شخص لديه إذن الوصول إلى المجلد الرئيسي الوصول إلى ملفك السري! ولتفادي ذلك، انقل ملفك السري إلى موقع جديد، خارج هيكل المجلد الأكبر الذي تمت مُشاركته.
- بمجرد مشاركة الملف، قد يُتاح لك خيار **عمل نسخة** و / أو **نقل** الملف إلى موقع آخر. لا تنقل ملف مُطلقًا دون إذن من مالكه!
- إذا كنت بحاجة إلى رؤية الملف في ملفاتي أو في موقع ثانوي، فإن أفضل ممارسة هي استخدام خيار أضف اختصارًا إلى Drive .
- إذا تم عمل نسخة من الملف، أو نُقل الملف، فاعلم أنه لن يكون له نفس الأذونات التي للملف الأصلي إلا إذا قمت بتعيين هذه الأذونات من جديد.

لا يغطي هذا الدليل مشاركة الملفات عبر محركات أقراص جوجل المُشتركة، أو المنصات الخارجية لمشاركة الملفات. لمعرفة المزيد حول هذه ، تفضَّل بزيارة أفضل الممارسات لمُشاركة الملفات عبر جوجل أو إدارة صفحة مساحات الأقراص المُشتركة. تتوفر كل صفحة من هذه الصفحات بعدة لغات: قم بالتمرير إلى أسفل الصفحة لتحديد لغتك.

أفضل طريقة للتحكم في الوصول إلى الملفات باستخدام Drive هي إنشاء مجموعة جوجل، وتعيين أذونات لأعضاء المجموعة. إن مجموعات جوجل ليست مخصصة فقط لإرسال رسائل البريد الإلكتروني، ولكنها أدوات قوية ومريحة لإدارة أذونات المجلدات والملفات. اكتشف المزيد حول مجموعات جوجل.

إذا كان مشروعك يتطلب استخدام تطبيقات خارج G Suite ، فشجع فريقك على التنزيل جوجلDrive لسطح المكتب. يتيح لك هذا البرنامج عرض أي مستندات في ملفاتي أو محركات الأقراص المشتركة كما لو كانت موجودة على الكمبيوتر المحمول ، حتى في حالة عدم الاتصال بالإنترنت ، ودون الحاجة إلى تنزيل العنصر أو تحويله إلى تنسيق جوجل.

مساعدة إضافية

يجب أن يكون التخطيط لجمع البيانات الحساسة أو استخدامها جزءًا لا يتجزأ من استراتيجية أكبر لدورة حياة البيانات لبرنامج أو نشاط ما. توجد العديد من الموارد التي من شأنها مُساعدتك في هذا الصدد.

- دليل بيانات الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر *(IFRC)*وهو مورد ممتاز للتمارين، وخطط الجلسات، وقوائم المراجعة، وغيرها من المواد الأخرى التي تُساعدك على تنظيم المحادثات والأنشطة مع فريقك لتطوير أنشطة البيانات المسؤولة. وعلى وجه الخصوص، الوحدة 7 - مُشاركة البيانات هي الوِحدة المُثلى للبدء منها.
- دليل اللجنة الدولية للصليب الأحمر لحماية البيانات في العمل الإنساني وهو دليل مفصل لكل جانب من جوانب البيانات الإنسانية تقريبًا. يتناول الفصل 2 تحديدًا مُشاركة البيانات.
- إن مجموعة أدوات شراكة التعلم النقدي لمسؤولية البياناتمُصممة على وجه التحديد لمُستخدمي النقد والقسائم، ولكنها معيار ذهبي في توجيه البيانات المسؤولة. انظر بشكل خاص ، ورقة النصائح # 6 و "مُشاركة البيانات". مجموعة الأدوات متاحة بالإنجليزية و العربية و الفرنسية ، و الأسبانية.

إزالة تعريف البيانات

يقدم هذا الدليل مثالاً على معلومات التعريف الشخصية (PII) من مجموعة البيانات. هناك عدة طرق "لإزالة التعريف" البيانات ، والتي تشير إلى أنشطة أو طرق لمعالجة البيانات التي تعمل على حماية هوية صاحب البيانات من الكشف عنها. هناك نوعان شائعان من إزالة التعريف وهما "إخفاء وتجهيل الهوية" و "استخدام الأسماء المستعارة".

إخفاء وتجهيل الهوية هي العملية التي يتم من خلالها جعل البيانات الشخصية مجهولة الهوية بحيث لا يمكن التعرّف على الفرد (أو "صاحب البيانات "): إنها عملية تغيير دائم للبيانات. تتضمن الطرق المعتادة للقيام بذلك حذف كميات معينة من البيانات الشخصية أو تطبيق مجموعات بعينها من البانات الشخصية.

مثال: تخيل أن منظمة ما لديها بيانات استقصاء تحتوي على حقول للاسم، ورقم الهوية الوطنية، واسم القرية، والانتماء العرقي، والعمر ومستوى التعليم، والمؤشرات الصحية. ففي هذه الحالة ، ستكون إزالة الاسم ورقم الهوية الوطنية هي الخطوة الأولى في جعل البيانات مجهولة لأن هذه "الصِفات المباشرة" هي بيانات شخصية تحدد هوية الفرد بشكل مباشر. وتظل "الصِفات غير المباشرة" كاسم القرية والانتماء العرقي والعمر ومستوى التعليم والمؤشرات الصحية كما هي.

ومع ذلك ، ورغم أن بعض البيانات تبدو "مجهولة" إلا أنها قد لا تكون كذلك. فإذا أجريّ المسح في قرية صغيرة جدًا حيث يتم تحديد اثنين فقط من السكان على أنهما انتماء عرقي معين ، وكان كل منهما من أعمار مُختلفة، فإن استخدام هاتين الصِفتين غير المُباشرتين قد يُساعِدا على تحديد هوية هؤلاء الأفراد! تُعرف العملية التي يتم من خلالها فحص جميع الصِفات لتقليل مخاطر إعادة تعريف صاحب البيانات باسم مراقبة الإفصاح الإحصائي. والخطوة الأولى في هذه العملية هي تقييم مخاطر الإفصاح ولدى مركز البيانات الإنسانية برنامج تعليمي عبر الإنترنت لإجراء تقييم لمخاطر الإفصاح.

استخدام الأسماء المستعارة من ناحية أخرى ، يصف معالجة البيانات الشخصية بطريقة لا يمكن بعد الآن إسناد البيانات الشخصية إلى موضوع بيانات معين دون استخدام معلومات إضافية ، مثل الرمز الأساسي.

على سبيل المثال: تخيل أن الاستقصاء يحتوي على اسمك، وبريدك الالكتروني، وعُمرك، وجنسيتك، ومكان عملك. فإن استخدام الأسماء المستعارة يأخذ البيانات التي يمكن التعرف عليك منها، وتحديدًا (اسمك ،وعنوان بريدك الإلكتروني، وعمرك) ويجعلها غير قابلة للوصول ومنفصلة عن البيانات غير المُعرَّفة للهوية ، مثل جنسيتك. ويمكن إعادة تجميع البيانات ذات الأسماء المستعارة معًا في وقت ما بحيث يمكن ربط جميع المعلومات مرة أخرى بمصدر أو شخص معين. هذا هو السبب في أن استخدام الأسماء المستعارة يتطلب الاحتفاظ بالمعلومات الإضافية بشكل منفصل، ويخضع للتدابير الفنية والتنظيمية لضمان عدم إسناد البيانات الشخصية إلى صاحب البيانات.

هل ينبغي أن تختار ما بين إخفاء وتجهيل الهوية أو استخدام الأسماء المستعارة ؟

عادة ما يكون إخفاء وتجهيل الهوية آمن ويُقلل من مخاطر التعرُّض لمعلومات التعريف الشخصية. ولكن، يُمكن أن يجعل هذا البيانات عامة لأقصى حد، مما يجعلها غير ملائمة للبرامج مثل المُساعدة النقدية والقسائم. من المهم في حالة البرامج الصِحية التي تنطوي على التطعيات، أو العلاجات الأخري التواصُل مع الأفراد لمتابعة العلاج. وفي كلتا هاتين الحالتين، يُعتبر اخفاء وتجهيل الهوية الخيار الافضل؛ لأنك تستطيع ارجاع البيانات معًا لتعريف الفرد عند الحاجة.

لا توجد إجابة واحدة صحيحة حول تفضيل طريقة على أخرى، ومن المهم فهم سبب جمع البيانات ، والمخاطر المحتملة المرتبطة بالاحتفاظ بهذه البيانات ، واحتياجات البرنامج ، قبل اختيار كيفية إزالة تعريف بياناتك.

من المهم أيضًا أن نفهم أن الأساليب المستخدمة لإخفاء هوية البيانات واختراق البيانات أصبحت أكثر تعقيدًا من أي وقت مضى وأن حتى البيانات غير المحددة الهوية ليست دائمًا آمنة بنسبة مائة بالمائة. في حالة وجود أي شكوك، اتصل بالفريق المختص بالبيانات، أو بفريق تكنولوجيا المعلومات للمساعدة.

☆ الأهمية

تُظهر اللجنة الدولية للصليب الأحمر ، ولجنة اختراق البريد الإلكتروني في الوكالة الأمريكية للتنمية الدولية ، ولجنة المشاركة غير الصحيحة للبيانات من قبل مفوضية الأمم المتحدة السامية لشؤون اللاجئين ، عدة طرق تتعرض فيها البيانات الإنسانية للخطر. تشكل البيانات المأخوذة من الاستقصاءات الأسرية، وتقييمات الاحتياجات، وأشكال أخرى من البيانات الجزئية حجمًا بالغ الأهمية من البيانات في قطاع العمل الإنساني. فهذه الأنواع من البيانات ضرورية لتحديد احتياجات ووجهات نظر المشاركين في البرنامج والمجتمعات التي نعمل فيها ، ولكنها تُمثل أيضًا مخاطر. كما يُعد فهم كيفية تقييم وإدارة حساسية هذه البيانات أمرًا بالغ الأهمية لضمان استخدامها بطريقة آمنة وأخلاقية وفعالة في سياقات الاستجابة المختلفة.

من بين مزايا استخدام البيانات الشخصية مجهولة المصدر ما يلي:

- الحماية ضد الافصاح غير الملائم عن البينات الشخصية؛
- وتطبيق قيود قانونية أقل على البيانات مجهولة المصدر؛ و
- السماح للمؤسسات بإنشاء بيانات مفتوحة أو متاحة للجمهور مع الاستمرار في الامتثال لالتزامات حماية البياناتهم.

المبادئ

إن إزالة تعريف البيانات جزءًا لا يتجزأ من معالجة البيانات ، ويجب أن تمتثل عملية معالجة البيانات الشخصية التي تقوم بها المنظمات الإنسانية للمبادئ التالية:

- **عدالة عملية المُعالجة وشرعيتها:** يجب أن تمتثل طُرق المُعالجة للتشريعات أو السياسات الإقليمية أو الوطنية أو المحلية التي قد تحد من البيانات التي يمكن إلغاء تعريفها، وكيفية استخدام تقنيات معينة. ينبغي أن تتسم أي معالجة للبيانات الشخصية بالشفافية بالنسبة لأصحاب البيانات المعنيين.
- **تحديد الغرض:** يجب على المنظمات الإنسانية تحديد وتوضيح الأغراض المحددة التي تُعالج البيانات من أجلها. ويجب أن تتسم هذه الأغراض بالوضوح والشرعية.
- **التناسب:** تأكد من أن كل نشاط مُتعلق بمعالجة البيانات الشخصية مُتناسب مع الهدف المعلن. على سبيل المثال: هل يُجمع الحد الأدنى من البيانات المطلوبة فقط؟
  هل توجد تدابير تقنية وتنظيمية ملائمة لتقليل المخاطر ذات الصلة بمعالجة البيانات؟
- **التغييرات التِقنيَّة:** تتغير مجموعات البيانات الجديدة، والأدوات الجديدة لتحليلها وتتقدم بسرعة، وبالمثل الوسائل التي يتم من خلالها اختراق البيانات أو سرقتها. لذلك من المهم فهم المخاطر الجديدة والناشئة التي قد تتعرض لها بياناتك، والاستمرار في تعديل أساليبك وممارساتك وفقًا لذلك.

استخدام الأسماء المستعارة

هذا مثال على إحدى طُرق إزالة تعريف البيانات في جدول بيانات. هناك مجموعة متنوعة من الوسائل لإجراء عملية إزالة التعريف، ويستخدم هذا المثال "الرمز الأساسي" لإزالة بيانات التعريف الشخصية الموجودة في المعرفات المباشرة والاحتفاظ بها في ملف منفصل. معلومات التعريف الشخصية (PII) هي المعلومات التي يمكن استخدامها لتحديد هوية الفرد. ومن الأمثلة الشائعة هي الاسم والعنوان ورقم الهاتف وتاريخ الميلاد ورقم الضمان الاجتماعي، أو رقم الهوية الوطنية.

التعليمات

يمكنك اتباع طريقة استخدام الأسماء المستعارة كمثال أساسي على استخدام الأسماء المستعارة لمجموعة بيانات. ويستخدم التمرين مجموعة بيانات نموذجية موجودة في مجلد البيانات الخاص بالدليل عبر الإنترنت.

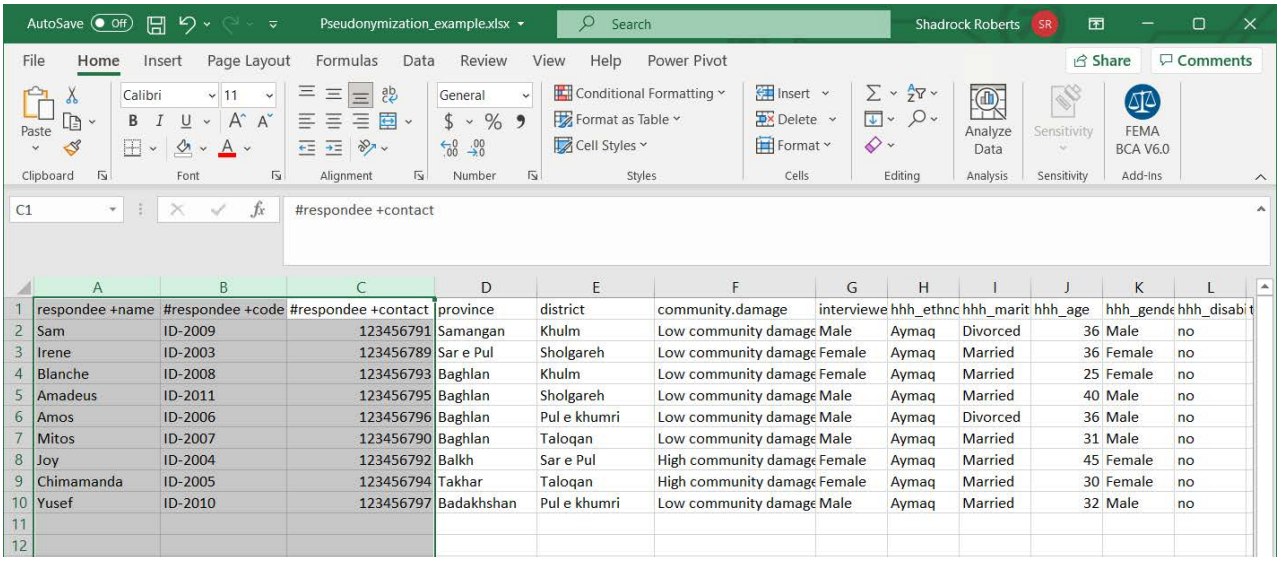
عند قيامك بتسمية بيانات المثال باسماء مستعارة، يمكنك متابعة البرنامج التعليمي لمركز البيانات الإنسانية لإجراء تقييم مخاطر الإفصاح.

الخُطوة -1 تحديد معلومات التعريف الشخصية

ابدأ بتحديد معلومات التعريف الشخصية في البيانات. وبطريقة مثالية، سيكون لديك بيانات وصفية - بيانات أو مستند تُعرِّف بياناتك - لمساعدتك على فهم الحقول التي تحتوي على معلومات التعريف الشخصية. وفي نموذج البيانات ، هناك ثلاثة أعمدة تحتوي على معلومات تعريف الشخصية محتملة:

- **# المُستجيب + الاسم** يبدو أنه يحتوي على اسم.
- **# المُستجيب + الرمز**من المحتمل أنه يحتوي على رقم تعريف من نوع ما.
- **#المُستجيب + جِهة الاتصال** من المُحتمل ان يحتوي على رقم هاتف محمول

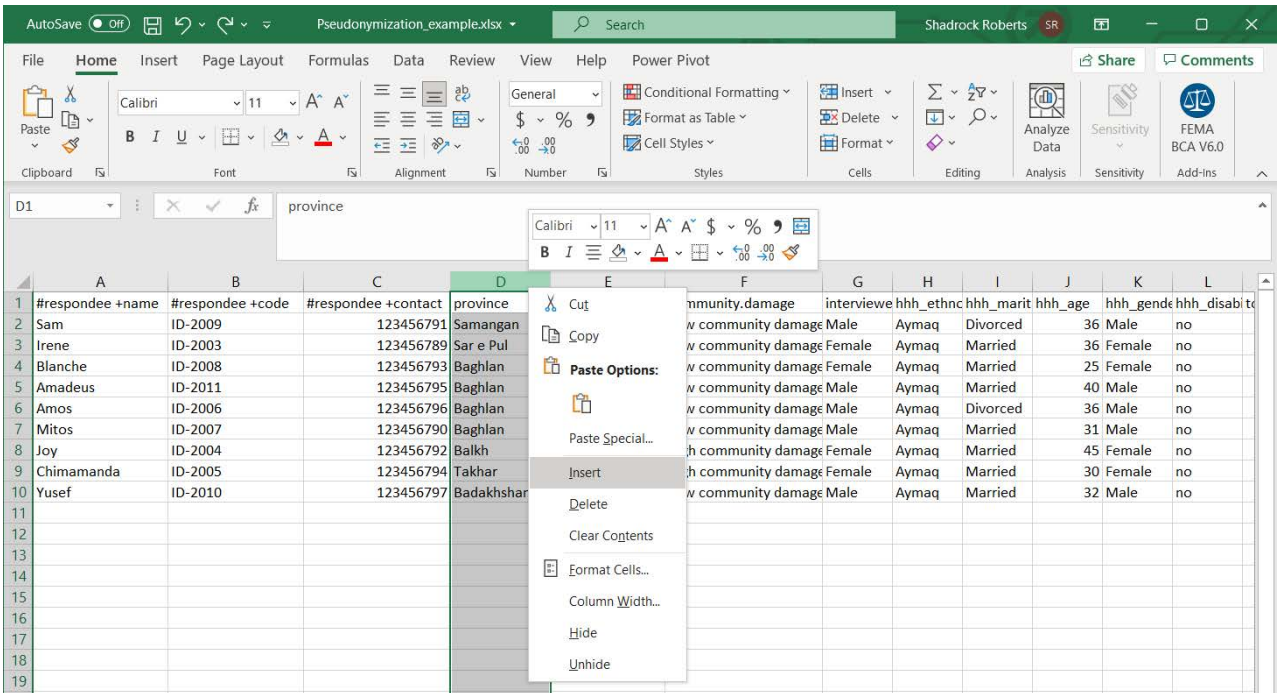
يستخدم كل من هذه المعرفات المباشرة لغة التبادل الإنساني لوضع علامات على البيانات.



	A	B	C	D	E	F	G	H	I	J	K	L
1	respondee +name	#respondee +code	#respondee +contact	province	district	community.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi t
2	Sam	ID-2009	123456791	Samangan	Khulm	Low community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan	Khulm	Low community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan	Sholgareh	Low community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan	Pul e khumri	Low community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan	Taloqan	Low community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh	Sar e Pul	High community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar	Taloqan	High community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshan	Pul e khumri	Low community damage	Male	Aymaq	Married	32	Male	no
11												
12												

الخطوة 2 - قُم بعمل أعمدة جديدة للرمز الأساسي

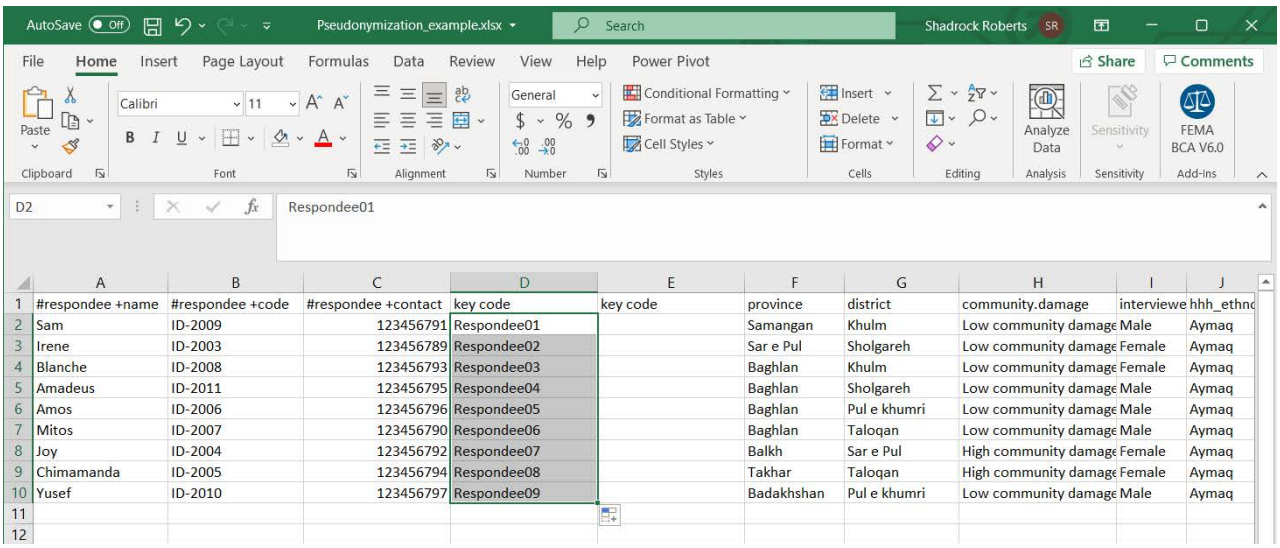
سنستخدم الرمز الأساسي - القيمة التي نحصُل عليها - لتقسيم معلومات التعريف الشخصية. نظرًا لأن المعرفات المباشرة مجمعة معًا ، فسننشئ عمودين جديدين بين الأعمدة C ، **# المُستجيب+ جهة الاتصال** والعمود D ، **المقاطعة**. نقوم بذلك في الإكسيل عن طريق تمييز عمود على يمين المكان الذي نريد إدراج أعمدة جديدة فيه، وننقر بزر الماوس الأيمن على العمود ونختار **إدراج**. كرر هذا الإجراء لعمل عمود آخر فارغ.



	A	B	C	D	E	F	G	H	I	J	K	L
1	#respondee +name	#respondee +code	#respondee +contact	province		mmunity.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan		w community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul		w community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan		w community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan		w community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan		w community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan		w community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh		h community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar		h community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshar		w community damage	Male	Aymaq	Married	32	Male	no
11												
12												
13												
14												
15												
16												
17												
18												
19												

الخطوة 3 -انشاء الرمز الأساسي

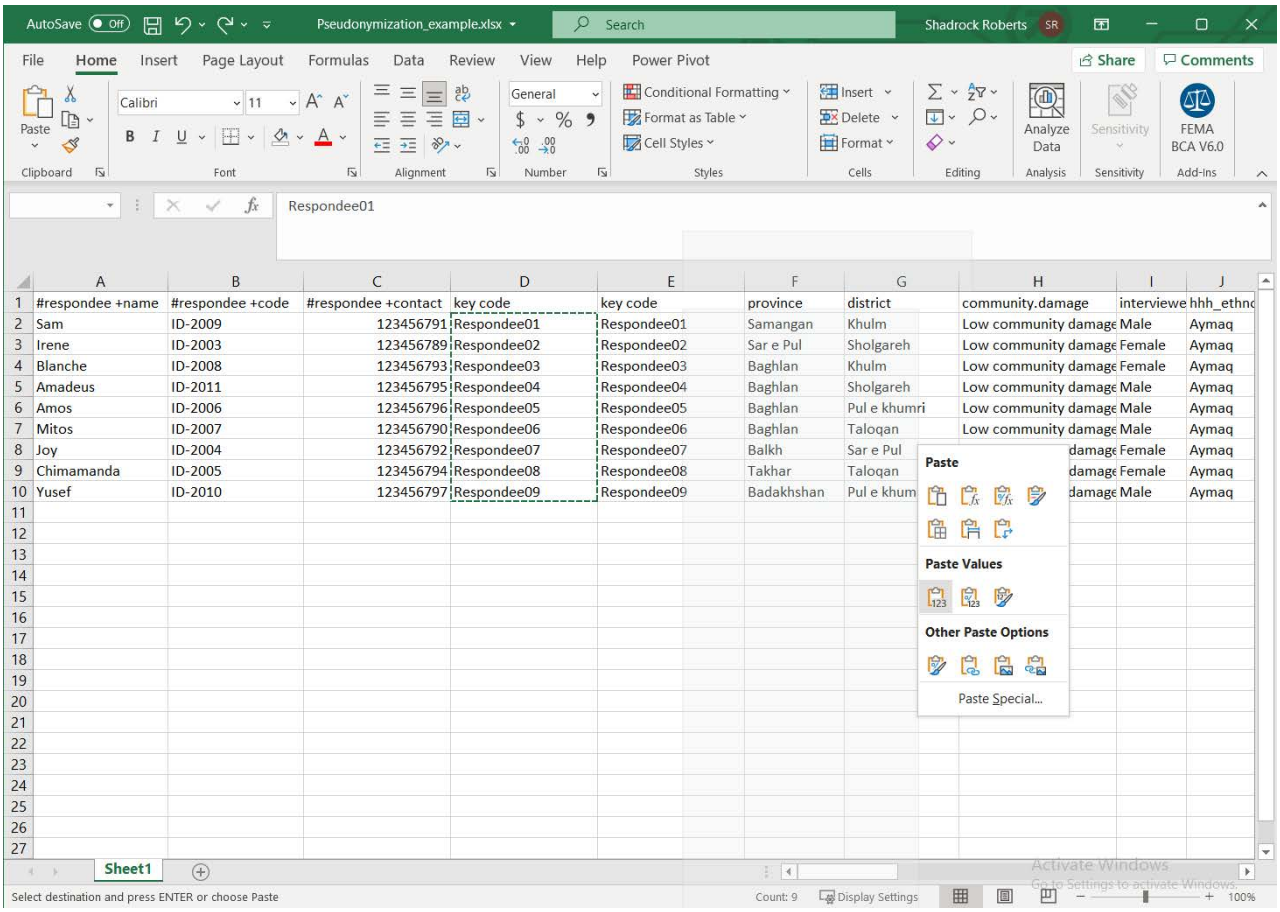
ابدأ بتسمية العمود الجديد. وسنستخد هُنا الاسم"الرمز الأساسي" في كل منهما: كل عمود سيتحتوي على نفس القيم. وهذا هو الوقت الأنسب لتحديث أي بيانات وصفية حول مجموعة البيانات هذه لشرح ما يعنيه**الرمز الأساسي**. وبعدها، سنستخدمخاصيةالتعبئة التلقائية في الإكسيل لإنشاء رمز بسيط. أكتب **Respondee01** في أول خلية. ثُم حدد تلك الخلية، وانقر على علامة السحب في الزاوية اليمنى السفلية للخلية ، واسحبها لأسفل حتى نهاية مجموعة البيانات. سيؤدي هذا تلقائيًا إلى تعبئة الرقم النهائي لكل سجل بحيث يُصبح لكل مستجيب رمز جديد.



	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethnc
2	Sam	ID-2009	123456791	Respondee01		Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02		Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03		Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04		Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05		Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06		Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07		Balkh	Sar e Pul	High community damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08		Takhar	Taloqan	High community damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09		Badakhshan	Pul e khumri	Low community damage	Male	Aymaq
11										
12										

الخطوة 4 -تكرار الرمز الأساسي، وإزالة المُعادلات

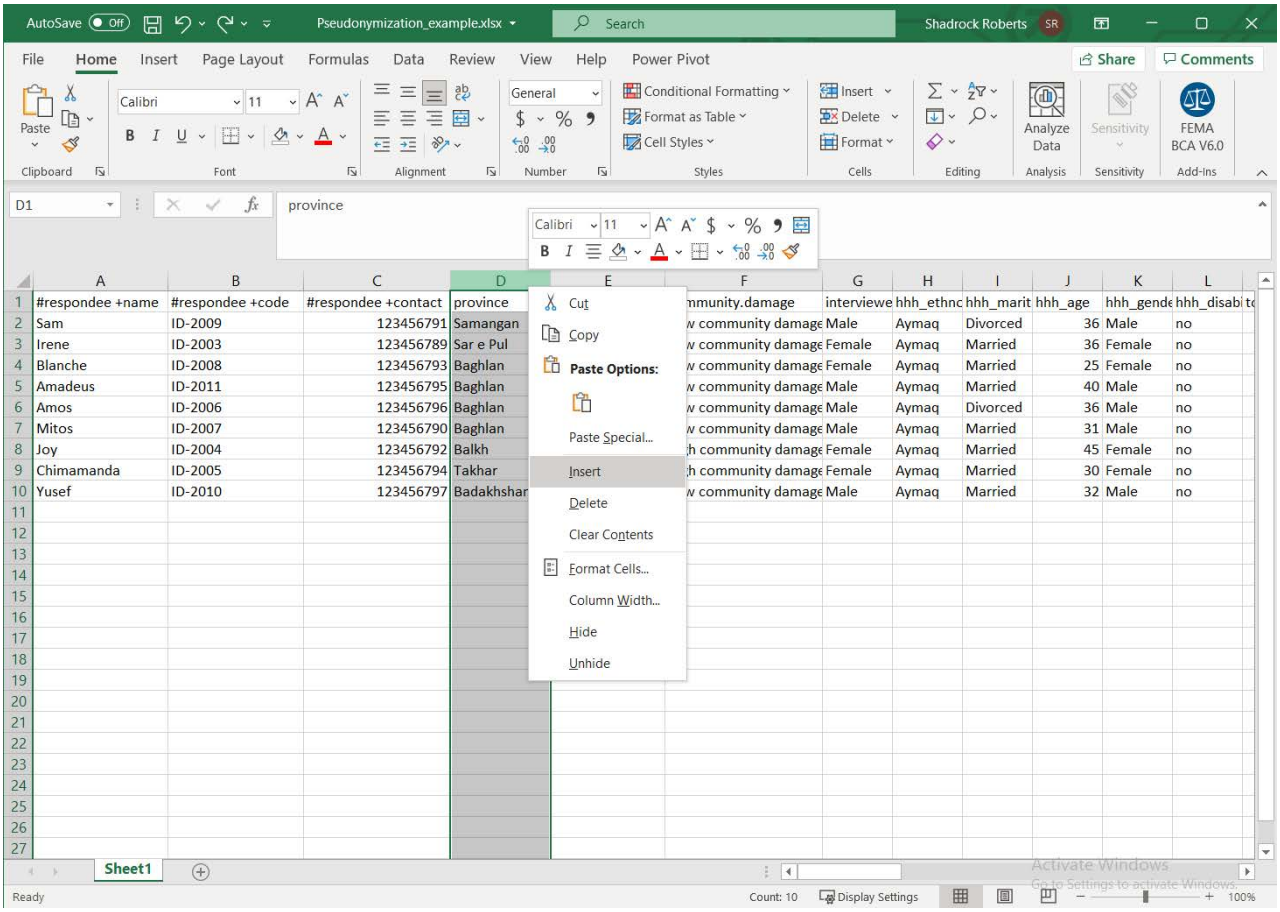
سنقوم الآن بنسخ الرمز الأساسي ولصقه في العمود المجاور. يمكنك القيام بذلك باستخدام أوامر لوحة المفاتيح الأساسية مثل **ctrl + C** أو حدد الخلايا التي تريد نسخها ، والنقر بزر الماوس الأيمن عليها، واختر**نسخ**. في العمود المجاور ، حدد الخلايا التي تريد لصق الرمز الساسي الجديد فيها ، وانقر بزر الماوس الأيمن واختر **لصق**. لقد اخترت تحديدًا لصق القيم فقط. وإذا استخدمت دالة لإنشاء رمز جديد ، فسيكون من المهم الاحتفاظ بها القيم فقط لاستخدامها كرمز أساسي!



	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethn
2	Sam	ID-2009	123456791	Respondee01	Respondee01	Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02	Respondee02	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03	Respondee03	Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04	Respondee04	Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05	Respondee05	Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06	Respondee06	Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07	Respondee07	Balkh	Sar e Pul	damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08	Respondee08	Takhar	Taloqan	damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09	Respondee09	Badakhshan	Pul e khum	damage	Male	Aymaq

الخطوة 5 - الفصل بين المعرفات المباشرة وغير المباشرة

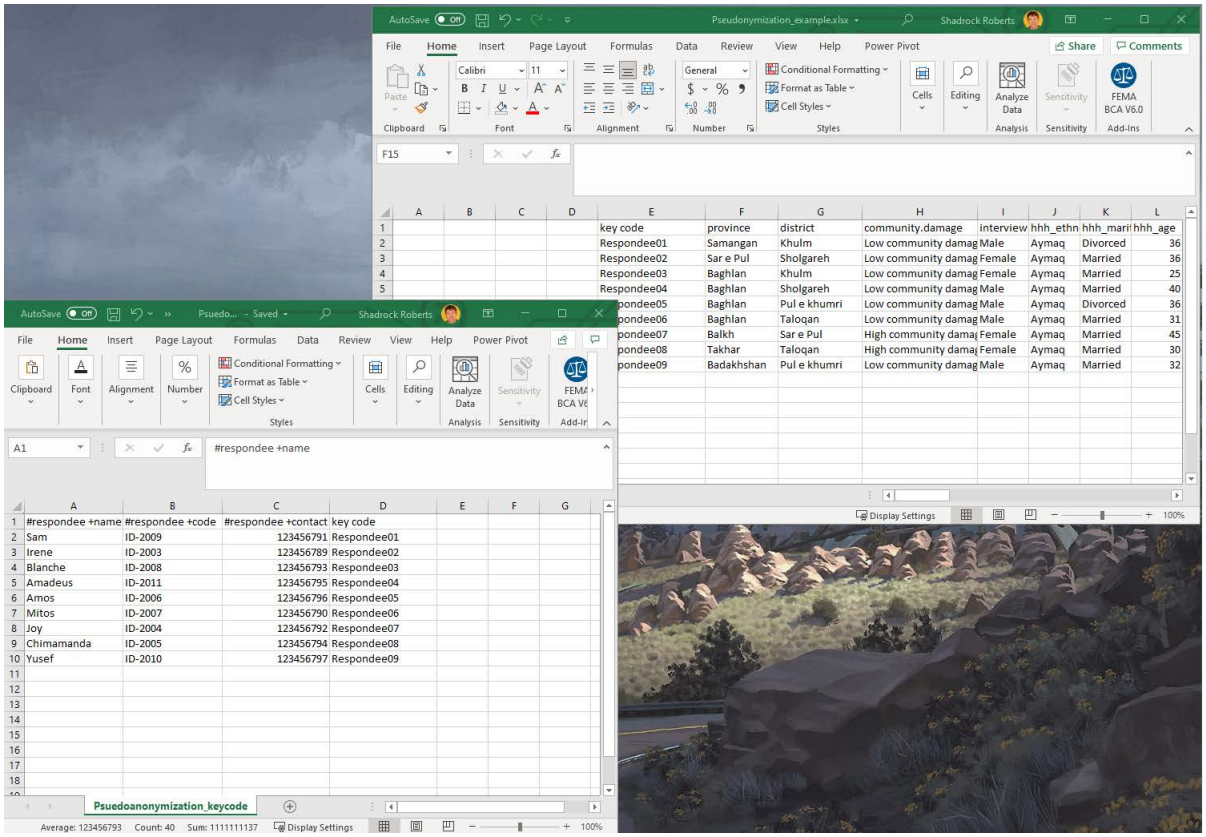
حدد الأعمدة التي تحتوي على المعرفات المباشرة لمعلومات التعريف الشخصيةوأحد أعمدة الرمز الرئيسي. في هذا المثال ، نُحدد الأعمدة منA إلىD . انقر بزر الماوس الأيمن عليهم واختر **قص**.



	A	B	C	D	E	F	G	H	I	J	K	L
1	#respondee +name	#respondee +code	#respondee +contact	province		mmunity.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan		w community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul		w community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan		w community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan		w community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan		w community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan		w community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh		h community damage	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar		h community damage	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshar		w community damage	Male	Aymaq	Married	32	Male	no
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												

وبعد ذلك ، افتح جدول بيانات جديد والصق فيه هذه القيم باستخدام اختصار لوحة المفاتيح **ctrl + V** ، أو أي طريقة أخرى. احفظ جدول البيانات الجديد.
لديك الآن جدولين للبيانات: يحتوي أحدهما على المعرّفات غير المباشرة، بينما تحتوي الورقة الجديدة على المعرّفات المباشرة ومعلومات التعريف الشخصية.
تحتوي كلتا مجموعتي البيانات على رمز أساسي لكل سجل من سجلات البيانات بحيث يمكن إعادة تجميع جميع البيانات عند الضرورة.

الخطوات التالية



يحتوي كلا الملفين على رمز أساسي يسمح بإعادة تجميعهما معًا. وتتمثل إحدى طرق القيام بذلك في الإكسيل، في استخدام دالة VLOOKUP لتعبئة الخلايا تلقائيًا بناءً على قيمة الخلايا الأخرى. وفي هذه الحالة ، يمكنك تعبئة الخلايا الفارغة في الملف الأصلي بمعلومات التعريف الشخصية المفقودة بناءً على قيمة **رمز الأساسي**.

يجب تخزين الملف الجديد يحتوي على المعرفات المباشرة، والتي تحتوي على معلومات التعريف الشخصية ، في مكان آمن. من الطُرق الممتازة للقيام بذلك هي تشفير الملف واستخدام التخزين السحابي لتحديد من يمكنه الوصول إلى الملف (**راجع ارشادات أفضل ممارسات التشفير ومشاركة الملفات**).

تذكر: في حين أنه تم تحديد جدول البيانات الأصلي عن طريق إزالة المعرفات المباشرة التي تحتوي على معلومات التعريف الشخصية الواضحة ، فإن المعرفات غير المباشرة الأخرى يُمكن دمجها مع بيانات أخرى أو تحليلها بطريقة تسمح بتحديد هوية الفرد.

ولهذا السبب ، يجب تخزين كلا الملفين بشكل آمن. إذا كنت ترغب في مشاركة الملف الأصلي - ليس ملف معلومات التعريف الشخصية - فسيكون من الضروري إجراء تقييم مخاطر الإفصاح لضمان الحد الأدنى من مخاطر إعادة تعريف البيانات. مركز البيانات الإنسانية لديه برنامج تعليمي عبر الإنترنت لإجراء تقييم مخاطر الإفصاح باستخدام برنامج إحصائي مفتوح المصدر "R". بالإضافة إلى ذلك، تُتيح صفحة مُختبر مكافحة الفقر لإلغاء التعريف لنشر البيانات مناقشة ممتازة لإلغاء تعريف البيانات، وتتضمن نموذج للتعليمات البرمجية لبرنامج ستاتا الإحصائي . ومتاح داخليًا لموظفي ميرسي كور، مسودة إرشادات من T4D بها دوال إكسيل إضافية.

وأخيرًا ، تساعد كل هذه الخطوات معًا في التخفيف من مخاطر الكشف عن معلومات التعريف الشخصية ، لذلك يجب إدراجها في تقييم تأثير الخصوصية (PIA) (**راجع دليل تقييم تأثير الخصوصية**) حتى يفهم الآخرون كيفية حماية هذه البيانات.

مساعدة إضافية

تعد عملية تحديد البيانات جزءًا من ممارسات الإدارة الجيدة للبيانات، ودورة حياة البيانات الأكبر ، وهي الأنشطة العامة لجمع البيانات الفردية كجزء من برنامج أو استجابة. تعد الموارد التالية مواقع ممتازة للبدء منها في فهم أكثر نُضجًا لإدارة بياناتك بمسؤولية.

- إن مجموعة أدوات شراكة التعلم النقدي لمسؤولية البياناتمُصممة على وجه التحديد لمُستخدمي النقد والقسائم، ولكنها معيار ذهبي في توجيه البيانات المسؤولة. مجموعة الأدوات متاحة بالإنجليزية و العربية و الفرنسية ، و الأسبانية.
- تُتيح شبكة عمل تعلم التحويل النقدي الإلكتروني مجموعة أدوات بدء البيانات للموظفين الميدانيين في المجال الإنساني يوفر سلسلة من أوراق النصائح الخاصة بالبيانات لفهم الجوانب المختلفة لإدارة البيانات الجيدة وممارسات الحماية.
- دليل اللجنة الدولية للصليب الأحمر لحماية البيانات في العمل الإنساني وهو دليل مفصل لكل جانب من جوانب البيانات الإنسانية تقريبًا. يتناول الفصل 2 تحديدًا إزالة تعريف البيانات.
- دليلEngine Room لاختصاصي التنمية الحديثة نظرة عامة جيدة للبيانات في سياق أنشطة التنمية الدولية. يتناول قِسممُشاركة البيانات على وجه التحديد إزالة الهوية.

تشفير ملف

يتناول هذا القسم مثالًا أساسيًا تشفير ملف باستخدام خاصية مايكروسوفت المتوفرة على أجهزة حواسيب ميرسي كور. توجد مجموعة من العوامل التي يجب مراعاتها عند تشفير ملف ، ولكننا هنا نركز على استخدام كلمة مرور، وتشفير ملف واحد. انظر الروابط أدناه للتعرُّف على الموارد التي تتناول التشفير بشيء من التعمُق. من المفيد في هذا الدليل معرفة الاختلاف الدقيق بين "حماية كلمة المرور" و "التشفير".

تخيل الحماية بكلمة مرور وكأنها صندوق له قفل. عند حماية مُستندك "بكلمة مرور"، فكأنك تضع هذا المستند في صندوق إلكتروني وتغلقه بكلمة مرور: ومَن لديه كلمة مرور هو فقط الذي يمكنه فتح الصندوق. ولكن إن اخترت كلمة مرور ليست قوية جدًا ، أو إذا تشاركتها مع الشخص الخطأ ، فيمكن لأي شخص بسهولة الدخول إلى الصندوق ومشاهدة المُستند الخاص بك! وعلى خلاف ذلك ، يَستخدم التشفير خوارزميات معقدة لتشفير المعلومات ، الأمر الذي يتطلب وجود مفتاح لفك تشفير تلك المعلومات. تخيل هذا على أنه وضع مُستندك في خلال آلة لتمزيق الورق، وتلك الآلة تُحدد مفتاحًا خاصًا لإعادة تجميع المستند مرة أخرى.

وعند الجمع ما بين الحماية بكلمة المرور والتشفير ، فإنك تضاعف حمايتك بشكل فعال. فإذا نجح شخص ما في كسر كلمة مرور الصندوق الإلكتروني ، فسيكون قادرًا فقط على رؤية أجزاء الورق الممزقة ما لم يكُن لديه أيضًا المفتاح المناسب. جميع حواسيب ميرسي كور المحمولة مشفرة باستخدام Microsoft BitLocker. هذا يمنع أقراص حواسيب ميرسي كور المحمول من الإزالة، أو والوصول إليها عبر حواسيب أخرى.

☆ الأهمية

يعد التشفير أمرًا بالغ الأهمية؛ لأنه يساعد على ضمان خصوصية المعلومات وأمانها. فبدون تشفير ، يمكن لأي شخص لديه حق الوصول إليها اعتراضها وقراءتها. عند التفكير فيما إذا كنت تريد تشفير البيانات أم لا ، سل نفسك ، "ما المخاطر التي يتعرض لها المشاركون في برنامج ميرسي كور ، وموظفيها، وشركائها في حالة فقدان هذه البيانات أو سرقتها؟" لذلك فإن تشفير أي شيء يحتوي على معلومات تعريف شخصية أو معلومات حساسة يُعد من القواعد الأساسية والمهمة.

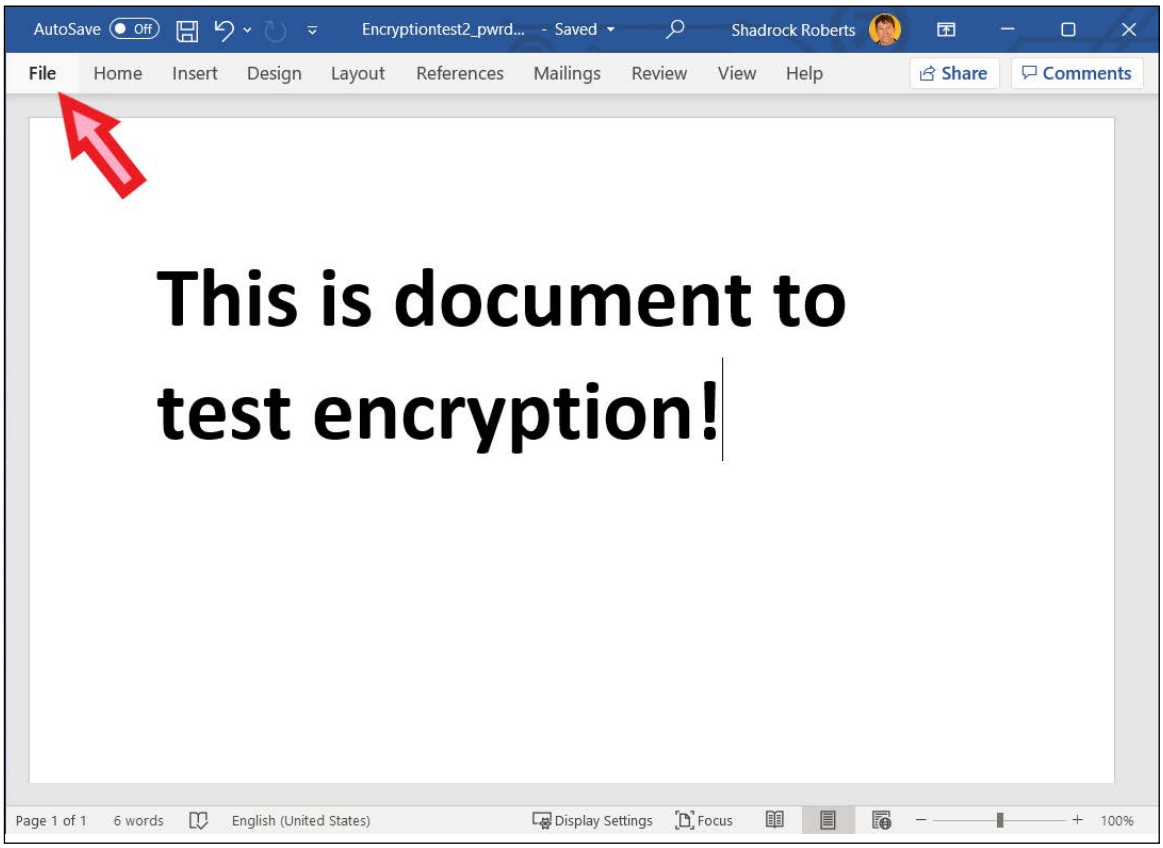
المبادئ

- استخدم أنظمة Mercy Corps المعتمدة لنقل البيانات المشفرة وتخزينها (مثل Microsoft SharePoint أو Google Drive). وعندما تكون في شك ، اطلب المشورة من فريق تكنولوجيا المعلومات المحلي.
- قُم بتشفير البيانات الحساسة في جميع مراحل جمعها واستخدامها ونقلها وتخزينها.
- استخدم كلمات مرور قوية، ولا تعيد استخدام كلمات المرور. يتم تداول قوائم كلمات المرور عبر الإنترنت مما يُسهِّل وصول شخص لديه إحدى كلمات المرور الخاصة بك إلى أكثر من حساب أو ملفات من ملفاتك الخاصة! قد ترغب في استخدام مدير لكلمات المرور ، مثل Lastpass. ومع ذلك، قد يكون مديرو كلمات المرور عرضة للهجوم الإلكتروني من قبل التطبيقات المزيفة ، لذلك من المهم أن يتم استخدام مديري كلمات المرور كجزء من نهج أوسع لتأمين البيانات.

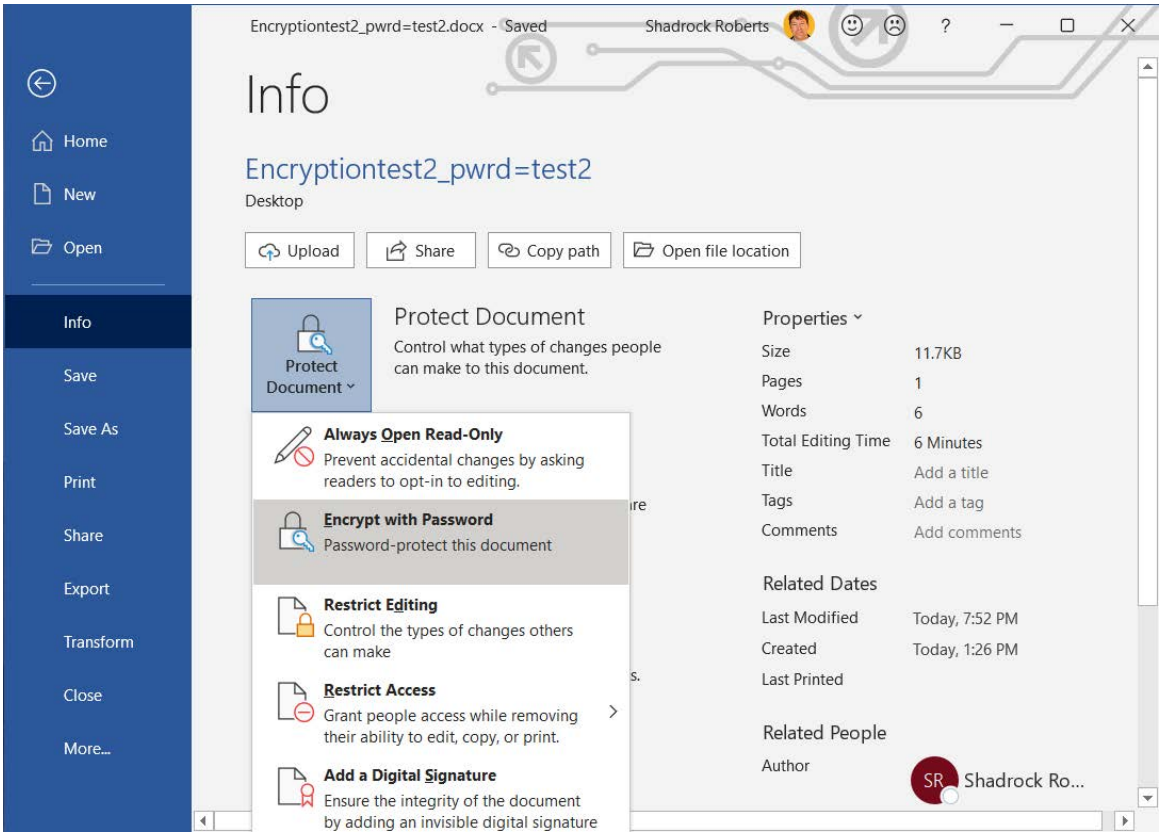
- في بيئة الفريق ، يكون التشفير فقط مثل أضعف رابط. فإذا فشل شخص واحد في استخدام التشفير ، فإن بيانات البرنامج الخاصة بك ستكون في خطر. فمن المهم للغاية توصيل هذا إلى فريقك: التشفير ليس مجرد مسألة تقنية ، ولكنه تغيير في السلوك أيضًا.
- افهم القوانين التي تحكم التشفير في بلدك. تضع القوانين المحلية في عدد من البلدان (مثل السودان واليمن وباكستان) قيودًا على برامج التشفير. في حالة الشك ، اطلب المشورة من فريق تكنولوجيا المعلومات المحلي: بشكل عام سيعملون معك للتأكد من أن محرك الأقراص الثابتة بحاسوبك مشفر بشكل مناسب باستخدام Intune.

التعليمات

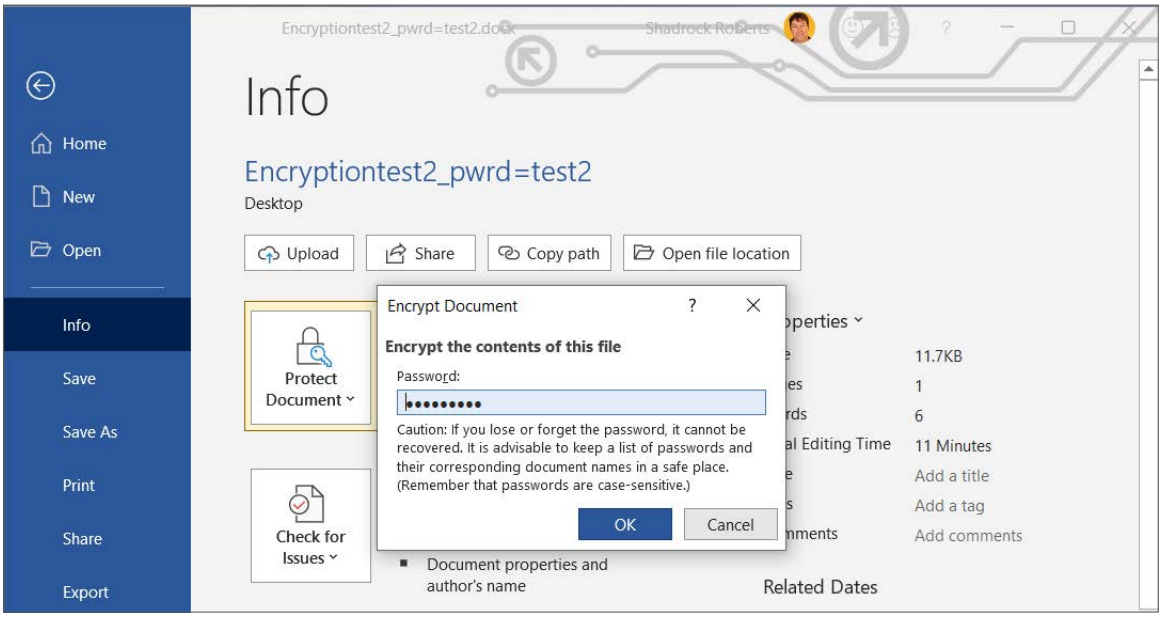
1 افتح ملف الوورد، أو الإكسيل، أو الباوربوينت الذي تريد تشفيره ومن القائمة اختر **ملف**.



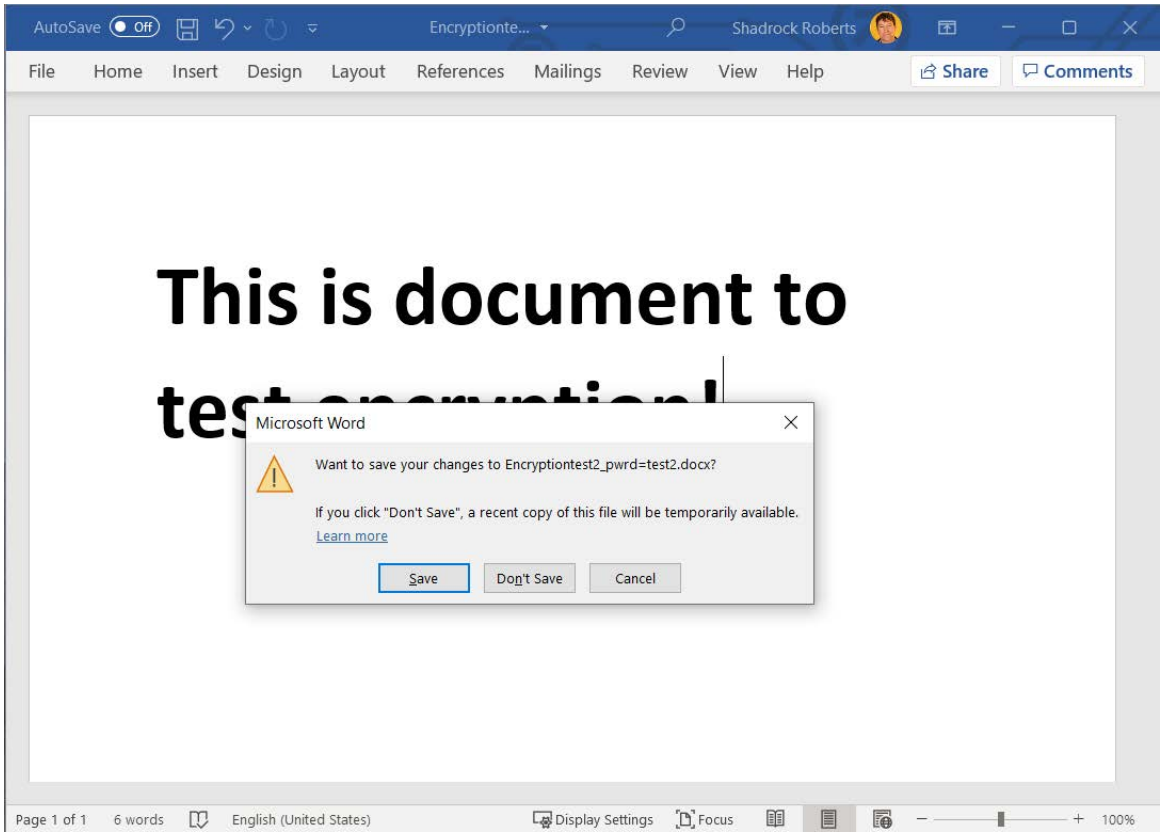
2 انتقل إلى **معلومات** > **حماية المستند** > **تشفير بكلمة مرور**.



3 اكتب كلمة مرور ، انقر فوق **موافق** ثم اكتبها مرة أخرى لتأكيدها.



4 احفظ الملف للتأكد من تفعيل كلمة المرور.



يمكنك الآن مشاركة الملف وكلمة المرور مع مَن يحتاجون إلى الوصول إليه. من أفضل الممارسات وضع الملف على خدمة سحابية معتمدة منميرسي كور مثل G Suite أو SharePoint. وتذكر ارسال رابط الملف وكلمة المرور بشكل منفصل. على سبيل المثال ، يمكنك مشاركة الملف باستخدام Google Drive (**راجع قسم مشاركة الملفات**) وعمل إشعار بأن الملف قد تمت مشاركته عبر جوجل، ثم مشاركة كلمة المرور عبر بريد إلكتروني مع زميل.

مساعدة إضافية

- توفر مجموعة بدء المعلومات لشبكة عمل تعلم التحويل النقدي الإلكتروني ورقة نصائح خاصة بالتشفير(أنظر صفحة النصائح#5)
- توفر مُنظمة Electronic Frontier بيانات تفصيلية حول مختلف أشكال التشفير.
- يتضمن دليل Engine Room لاختصاصي التنمية الحديثة قسمًا حول إدارة البيانات، كما يوفر أ أيضًا فكارًا إضافية عالية المستوى حول التشفير.

جِهات الاتصال

هيثير لاف
مدير حماية البيانات العالمية والخصوصية | تكنولوجيا المعلومات
hlove@mercycorps.org

شادروك روبرتس
أخصائي حماية البيانات | تكنولوجيا المعلومات
shroberts@mercycorps.org

نُبذة عن ميرسي كور

ميرسي كور هي منظمة عالمية رائدة يُحركها الإيمان بإمكانية خلق عالم أفضل. ففي حالات الكوارث والمِحن، وفي أكثر من 40 دولة حول العالم ، نتشارك نضع الحلول الجريئة حيز التنفيذ— لمساعدة الناس على التغلُّب على المِحن وبناء مجتمعات أقوى من الداخل.
الآن ، وفي المستقبل.

MERCY CORPS

مقرات العمل العالمية
SW Ankeny Street 45
Portland, Oregon 97204
888.842.0842
mercycorps.org

المقر الأوروبي
Sciences 40
Edinburgh EH9 1NJ
Scotland, UK
+44.131.662.5160
mercycorps.org.uk