

Anhang 2
Technische und Operative Maßnahmen (einschließlich Sicherheitsanforderungen)

Organisatorische Sicherheitsvorkehrungen

- Der Anbieter muss eine Geheimhaltungsvereinbarung unterzeichnen, die anschließend von einer IPSOS-Führungskraft mitunterzeichnet werden muss, bevor ihm Zugang zu den Daten und/oder der Umgebung von Ipsos gewährt wird.
- Der Anbieter hat Mitarbeiter benannt, zu deren Aufgaben der Datenschutz und die Informationssicherheit gehören.
- Der physische Zugang zum Gebäude wird durch verschiedene Zugangskontrollmechanismen (z. B. Schlüsselkarten) beschränkt, und in den meisten Fällen sind die Eingänge zu den Büros des Anbieters mit Empfangsmitarbeitern/Sicherheitspersonal besetzt.
- Die Mitarbeiter des Anbieters werden bei Beginn ihrer Tätigkeit beim Anbieter in Datenschutz- und Informationssicherheitsfragen geschult und unterliegen der Geheimhaltungspflicht.
- Es ist den Mitarbeitern nicht gestattet, personenbezogene Daten auf einem Speichermedium (z. B. einer (externen) Festplatte, Disc oder Stick) zu speichern, um in Räumlichkeiten, die nicht vom Anbieter kontrolliert werden, erneut auf die Informationen zugreifen zu können.
- Werden personenbezogene Daten in Papierform aufbewahrt, müssen alle Mitarbeiter, die mit solchen personenbezogenen Daten umgehen, eine „Clear Desk Policy“ befolgen, damit keine personenbezogenen Daten während ihrer Abwesenheit unbeaufsichtigt bleiben. Personenbezogene Daten in Papierform werden sicher aufbewahrt, um unbefugten Zugriff zu verhindern.
- Es muss ein Business-Continuity-Plan erstellt und jährlich getestet werden.

Risikomanagement im Bereich Informationssicherheit

- Der Anbieter muss regelmäßig die Risiken innerhalb der Informationstechnologie bewerten, insbesondere in Bezug auf Vermögenswerte, die mit den an Ipsos gelieferten Dienstleistungen/Produkten in Verbindung stehen oder daran beteiligt sind. Das implementierte Risikomanagement-Framework sollte den Anforderungen der Normen ISO 27001, ISO 27002 oder ISO 31000 entsprechen.

Richtlinie zur Informationssicherheit

- Der Anbieter muss seine Richtlinien zur Informationssicherheit dokumentieren und Informationssicherheitsprogramme befolgen, die auf mindestens einem der folgenden Rahmenwerke basieren:
 - ISO 27001- und ISO 27002-Normen
 - NIST 800 Special Security Publications.
- Der Anbieter muss sein Sicherheitsprogramm einem der oben genannten Sicherheitsrahmen zuordnen und dabei sicherstellen, dass sein Informationssicherheitsprogramm keine Lücken aufweist.

Rahmenwerk für Informationssicherheit

- Der Anbieter muss die Zuständigkeit für die Überwachung der Entwicklung, Einführung, Durchsetzung und Einhaltung der Anforderungen, Richtlinien, Standards und Verfahren zur Informationssicherheit definieren, dokumentieren und zuweisen.
- Der Anbieter muss sicherstellen, dass die zugewiesene Rolle innerhalb der Organisation eine ausreichend hohe Einstufung hat, um die Aufgaben effektiv und unabhängig ausführen zu können.
- Um Interessenkonflikte zu vermeiden, muss der Anbieter sicherstellen, dass diese Rolle keine direkte Verantwortung für die Informationsverarbeitung und den Technologiebetrieb hat.

Vermögenswerte-Verwaltung

- Der Anbieter muss einen Prozess zur Verwaltung von Vermögenswerten, Systemen und Geräten („Vermögenswerte“) entwerfen, dokumentieren, implementieren und aufrechterhalten, der sich auf die Vermögenswerte des Anbieters erstreckt und die Möglichkeit bietet, die Abhängigkeiten zwischen den Vermögenswerten des Anbieters und denen von Ipsos – einschließlich der Informations-Vermögenswerte – abzubilden.
- Der Anbieter muss eine bestimmte Person benennen, die für alle Vermögenswerte des Anbieters verantwortlich ist, die auf Vermögenswerte und Daten von Ipsos zugreifen.
- Der Anbieter muss Regeln für die zulässige Nutzung von Vermögenswerten Dritter, einschließlich, aber nicht beschränkt auf Vermögenswerte und Daten von Ipsos, dokumentieren und umsetzen.
- Die Regeln für die zulässige Nutzung müssen vorschreiben, dass Vermögenswerte Dritter nicht für Aktivitäten verwendet werden dürfen, die als unzulässig identifiziert wurden.
- Die Regeln für die zulässige Nutzung müssen vorschreiben, dass Vermögenswerte Dritter auf professionelle, rechtmäßige und ethische Weise genutzt werden müssen.
- Wenn der Anbieter eine Verbindung zu Vermögenswerten von Ipsos (einschließlich Servern, Workstations, Infrastruktur, Internet-Gateway oder Netzwerk) herstellt oder diese nutzt, muss er alle geltenden Nutzungsbedingungen, Richtlinien, Standards und Verfahren von Ipsos einhalten.
- Der Anbieter ist verpflichtet, die Vermögenswerte von Ipsos zu schützen und umsichtig zu nutzen, und wird bei der Nutzung der Vermögenswerte von Ipsos, einschließlich der Systeme, Computer, Telefone, Internetzugänge, E-Mail-Konten, Voicemail-Konten, Kopierer, Faxgeräte, Fahrzeuge oder sonstigen Eigentums von Ipsos, mit gesundem Menschenverstand und Diskretion vorgehen.
- Der Lieferant darf ohne die vorherige schriftliche Genehmigung von Ipsos niemals Geräte oder Vermögenswerte, die nicht Eigentum von Ipsos sind, mit dem Netzwerk von Ipsos verbinden.

- Ipsos muss alle Anträge von Unternehmen bezüglich der Verbindung von nicht-Ipsos-eigenen Vermögenswerten mit dem Netzwerk von Ipsos vor der Erteilung einer solchen Genehmigung prüfen.
- Vermögenswerte, die mit dem Netzwerk von Ipsos verbunden sind, müssen den Sicherheitsrichtlinien, Standards, Betriebsverfahren und Kontrollen von Ipsos entsprechen, einschließlich, aber nicht beschränkt auf Konfiguration, Absicherung, Patching, Zugriffskontrolle und Virenschutzprozesse.

Sicherheit im Personalwesen

Der Anbieter muss:

- sicherstellen, dass alle Mitarbeiter des Anbieters, Anbieter und Unterauftragsverarbeiter, die auf Vermögenswerte von Ipsos zugreifen, vor ihrer Einstellung überprüft werden. Die Überprüfung muss Strafregister-, Finanz- und Beschäftigungshintergrundüberprüfungen umfassen, sofern dies nicht im Widerspruch zu den geltenden Rechtsvorschriften steht.
- Richten Sie Prozesse ein, um Mitarbeiter während ihrer Beschäftigung regelmäßig zu überprüfen, ob sie Zugriff auf regulierte, vertrauliche oder personenbezogene Daten haben.
- Stellen Sie sicher, dass alle Personen, die Zugang zu Ipsos-Assets haben, an einer Sensibilisierungskampagne zum Thema Informationssicherheit teilnehmen. Die Kampagne muss die Mitarbeiter über ihre Verantwortung für die Sicherheit der Ipsos-Assets aufklären.
- Stellen Sie sicher, dass alle Benutzer-IDs, Tokens oder physischen Zugangsausweise einem bestimmten Mitarbeiter des Lieferanten oder Unterauftragsverarbeiters des Lieferanten zugewiesen sind.
- Stellen Sie sicher, dass alle Benutzer-/System-/Dienst-/Administratorkonten und Passwörter niemals weitergegeben werden.
- Benachrichtigen Sie Ipsos unverzüglich schriftlich, wenn ein Mitarbeiter oder Unterauftragsverarbeiter des Anbieters nicht mehr für das Ipsos-Konto tätig ist oder die ID-Berechtigung für von Ipsos verwaltete Vermögenswerte und Daten geändert werden muss. Die Benachrichtigung muss den Namen, die Benutzer-ID und alle Konten enthalten, auf die die Person Zugriff hatte oder deren Passwort sie kennt.

Physische und umgebungsbezogene Sicherheit

Der Anbieter muss alle erforderlichen Informationssicherheitskontrollen implementieren, um sicherzustellen, dass alle Vermögenswerte des Anbieters, die an den für Ipsos erbrachten Dienstleistungen beteiligt sind, sowie alle Vermögenswerte von Ipsos, die sich in der Obhut des Anbieters befinden, vor folgenden Gefahren geschützt sind:

- Naturkatastrophen,
- Diebstahl, physischem Eindringen, unrechtmäßigem und unbefugtem physischem Zugriff,
- Problemen mit der Belüftung, Heizung oder Kühlung, Stromausfällen oder -unterbrechungen.

Betriebsmanagement

Netzwerksicherheit: Der Anbieter muss dort, wo regulierte, vertrauliche oder personenbezogene Daten von Ipsos verarbeitet werden, Dienste zur Verhinderung von Datenverlusten (Data Loss Prevention / „DLP“) und/oder zur Einbruchs-Überwachung einsetzen.

Der Anbieter muss sicherstellen, dass alle unnötigen Dienste, Ports und der gesamte Netzwerkverkehr auf allen IT-Systemen, die auf Ipsos-Ressourcen zugreifen, deaktiviert sind.

Systemsicherheit:

Der Anbieter muss über einen Prozess zur Anwendung und Verwaltung von Sicherheitsupdates, Patches, Fixes und Upgrades (zusammenfassend als „Patches“ bezeichnet) auf allen IT-Systemen des Anbieters verfügen.

- Der Anbieter muss sicherstellen, dass Patches, die Sicherheitskorrekturen oder Sicherheitsupdates enthalten, innerhalb von 20 Tagen nach ihrer Veröffentlichung für alle IT-Systeme des Anbieters, die auf vertrauliche, personenbezogene oder regulierte Daten von Ipsos zugreifen, getestet und bereitgestellt werden.
- Andernfalls muss der Anbieter sicherstellen, dass Patches innerhalb von 30 Tagen nach ihrer Veröffentlichung bereitgestellt werden.
- Alle Ausnahmen sind zu dokumentieren, wobei der Grund für die Nichtbereitstellung der genannten Patches anzugeben ist.

Der Anbieter muss sicherstellen, dass auf allen IT-Systemen, die auf Vermögenswerte und Daten von Ipsos zugreifen, Programme zum Schutz vor Malware, Viren, Trojanern und Spyware installiert sind; diese müssen über die neuesten und aktuellen Signaturen, Definitionsdateien, Software und Patches des Herstellers verfügen.

Der Anbieter muss sicherstellen, dass alle ungenutzten oder unnötigen Softwareprogramme, Anwendungen, Dienste, Beispiel-/Standarddateien und Ordner auf allen IT-Systemen, die auf Vermögenswerte und Daten von Ipsos zugreifen, deaktiviert sind.

Betriebssicherheit – Der Anbieter muss:

- sicherstellen, dass Änderungen an IT-Systemen, die für Ipsos arbeiten, keine negativen Auswirkungen auf die Sicherheit haben.
- Dokumentierte Verfahren und Prozesse für das Änderungsmanagement befolgen.
- Regulierte, personenbezogene oder vertrauliche Informationen nicht in eine Nicht-Produktionsumgebung oder an einen unsicheren Ort verschieben oder übertragen.

Notfallwiederherstellung

- Der Anbieter hat geeignete Maßnahmen zur Notfallwiederherstellung implementiert, um sicherzustellen, dass die von ihm verarbeiteten personenbezogenen Daten im Falle eines Verlusts oder einer Zerstörung dieser Daten wiederhergestellt werden können.

- Der Notfallwiederherstellungsplan, mit dem die Notfallwiederherstellungsmaßnahmen umgesetzt werden, definiert RTO (Recovery Time Objectives) und RPO (Recovery Point Objectives). Die RPO und RTO werden Ipsos innerhalb von 20 Werktagen nach Vertragsunterzeichnung im Rahmen des Notfallwiederherstellungsplans mitgeteilt.
- Der Anbieter überprüft diese technischen Sicherheitsvorkehrungen regelmäßig, um sicherzustellen, dass sie angesichts der von ihm verarbeiteten Daten und des technologischen Fortschritts weiterhin geeignet sind.

Datenmanagement

Datensicherheit

Der Anbieter muss:

- starke Verschlüsselungsschlüssel-Verwaltungsverfahren anwenden, um die Verfügbarkeit verschlüsselter verbindlicher Informationen sicherzustellen
- alle Datenbestände von Ipsos bei der Übertragung zwischen dem Anbieter und Ipsos sowie zwischen dem Anbieter und allen anderen Dritten verschlüsseln, wenn es sich bei den übertragenen Daten um Daten von Ipsos handelt.
- Verschlüsseln Sie vertrauliche Informationen von Ipsos jederzeit; die Verschlüsselung muss mindestens dem Standard AES-256-Bit entsprechen.
- Bei Verwendung eines öffentlichen/privaten Verschlüsselungstools muss der Anbieter alle erforderlichen Maßnahmen zum Schutz des privaten Schlüssels ergreifen.
- Bei der Verschlüsselung von Ipsos-Daten dürfen Passwörter/Passphrasen nicht per E-Mail oder Voicemail versendet werden.
- Wenn ein Passwort/eine Passphrase zur Verschlüsselung des Dokuments verwendet wird, teilen Sie das Passwort/die Passphrase für das verschlüsselte Dokument außerhalb des Kommunikationskanals mit:
 - Persönlich
 - Live am Telefon

Übertragung von Daten

Akzeptable Methoden der Datenübertragung:

- Secure File Transfer Protocol (SFTP): SFTP ist eine verschlüsselte Version von FTP, die SSH verwendet, um Daten sicher zwischen Clients und Servern zu übertragen und so die Vertraulichkeit und Integrität der Daten zu gewährleisten.
- File Transfer Protocol Secure (FTPS): FTPS ist eine Erweiterung von FTP, die Unterstützung für die kryptografischen Protokolle Transport Layer Security (TLS) und Secure Sockets Layer (SSL) hinzufügt, um Daten während der Übertragung zu verschlüsseln.
- Hypertext Transfer Protocol Secure (HTTPS): HTTPS ist eine verschlüsselte Version von HTTP, die SSL/TLS verwendet, um die Kommunikation zwischen Webservern und Clients zu sichern.
- Virtual Private Network (VPN): Ein VPN erstellt einen sicheren, verschlüsselten Tunnel zwischen Geräten und ermöglicht so eine sichere Datenübertragung über öffentliche Netzwerke.
- Verschlüsselte E-Mails: Sichere E-Mail-Lösungen wie PGP (Pretty Good Privacy) oder S/MIME (Secure/Multipurpose Internet Mail Extensions) bieten eine End-to-End-Verschlüsselung und gewährleisten so die Vertraulichkeit der E-Mail-Kommunikation.
- Verschlüsselter Cloud-Speicher: Dienste wie Google Drive, Dropbox oder Microsoft OneDrive bieten sichere Datenübertragungsoptionen, indem sie Daten im Ruhezustand und während der Übertragung verschlüsseln und zusätzliche Sicherheitsstufen wie die Zwei-Faktor-Authentifizierung anbieten.
- Managed File Transfer (MFT): MFT-Lösungen bieten zentralisierte, sichere und überprüfbare Dateiübertragungen durch Verschlüsselung, Zugriffskontrollen und Überwachung, um Daten während der Übertragung und im Ruhezustand zu schützen.
- Remote Desktop Protocol (RDP) über SSL/TLS: Die Verwendung von RDP mit SSL/TLS-Verschlüsselung gewährleistet eine sichere Verbindung zwischen Remote-Clients und Servern und ermöglicht so die sichere Übertragung von Daten zwischen den Geräten.
- Sichere APIs und Webdienste: RESTful-APIs und Webdienste, die HTTPS, OAuth 2.0 und API-Schlüssel verwenden, können eine sichere Datenübertragung zwischen Clients und Servern gewährleisten. Diese Sicherheitsmaßnahmen stellen sicher, dass nur autorisierte Clients auf Daten zugreifen und diese bearbeiten können.
- Amazon Web Services (AWS) S3-Buckets: AWS S3 ist eine skalierbare Speicherlösung, die zur sicheren Speicherung und Übertragung von Daten verwendet werden kann. Standardmäßig sind S3-Buckets privat, und Daten können mithilfe von SSL-Verschlüsselung sicher übertragen werden. Zusätzliche Sicherheitsmaßnahmen wie Identitäts- und Zugriffsmanagementrichtlinien (IAM), Bucket-Richtlinien und Verschlüsselungsoptionen können implementiert werden, um die Daten weiter zu schützen.

Unzulässige Methoden der Datenübertragung:

- FTP (File Transfer Protocol)
- E-Mail
- Dateiübertragung durch Dritte Websites wie www.yousendit.com, www.sendbigfiles.com und www.mailbigfile.com

Umgang mit Daten

Nur diejenigen Mitarbeiter des Anbieters, die für das spezifische Ipsos-Projekt, für das die Stichprobe bestimmt ist, eingesetzt werden, dürfen die von Ipsos bereitgestellten Kundendaten verarbeiten.

- Der Anbieter muss die Genehmigung von Ipsos einholen, um die von Ipsos bereitgestellte Kundenstichprobe an andere Anbieter oder Unteranbieter weiterzugeben.
- Die Unterlieferanten des Anbieters müssen bei der Übertragung und Verarbeitung der von Ipsos bereitgestellten Kundenstichproben die gleichen Verfahren befolgen, wie sie in diesem Dokument beschrieben sind.

Speicherung von Daten

- Der Anbieter muss die von Ipsos bereitgestellten Kundenstichproben auf einem Server speichern, der physisch gesichert ist und auf den nur autorisierte Mitarbeiter Zugriff haben.
- Der Anbieter muss die von Ipsos bereitgestellten Kundenstichproben auf einem Server speichern, der durch eine Firewall geschützt ist und über die neuesten Betriebssystem- und Sicherheitspatches verfügt.
- Der Anbieter muss das Verzeichnis, in dem die von Ipsos bereitgestellten Kundenstichprobe gespeichert sind, weglassen. Damit soll vermieden werden, dass die von Ipsos bereitgestellten Kundenstichproben versehentlich über einen längeren Zeitraum auf den Sicherungsbändern des Anbieters gespeichert bleiben.

ODER

- Der Anbieter kann die von Ipsos bereitgestellten Kundenstichproben auf Sicherungsbändern sichern, sofern diese nur für die Notfallwiederherstellung verwendet und nicht aufbewahrt werden. Die Bänder müssen nach einer festgelegten Zeitspanne überschrieben werden.

Datenvernichtungsprozess

Der Anbieter muss sicherstellen, dass:

- Die funktionierenden Speichermedien entweder gelöscht, geschreddert, aufbewahrt oder entmagnetisiert werden;
- Nicht funktionsfähige Speichermedien wie folgt geschreddert, aufbewahrt oder entmagnetisiert werden:

Entmagnetisierung

In Regionen, in denen eine Entmagnetisierungsanlage vorhanden ist, werden alle Festplatten und magnetischen Medien wie Bänder vor der Entsorgung entmagnetisiert.

Festplatten und Speichermedien

- Funktionierende oder nicht funktionierende Festplatten oder elektronische Medien wie Bänder, die durch Schreddern, Entmagnetisieren oder Löschen vernichtet werden sollen, müssen an einem gesicherten Ort aufbewahrt werden, zu dem nur diejenigen Mitarbeiter Zugang haben, die Zugang zu den Medien benötigen.
- Es wird eine Liste der Personen geführt, die Zugang zu den Medien haben.
- Es wird eine Liste aller Festplatten und elektronischen Medien wie Bänder geführt und aktualisiert, wenn Festplatten und elektronische Medien hinzugefügt/vernichtet werden. Das Inventar enthält die Seriennummern der Festplatten und die Etiketten/Bezeichnungen der Bänder. Die Liste enthält auch den Status und Zustand der Festplatten.
- Dieses Inventar wird zweimal jährlich überprüft, um festzustellen, ob Festplatten und elektronische Medien verloren gegangen sind oder gestohlen wurden.

Standards für die Vernichtung von Medien

- Der Anbieter muss jederzeit nachweisen können, dass er die Kontrolle über unsere Informationsressourcen (d. h. Festplatten/Bänder) bis hin zu deren Vernichtung hat.
- Die Bestätigung der Vernichtung unserer Medien muss innerhalb des nächsten Werktags nach ihrer Entsorgung erfolgen.
- Festplatten werden in Partikel mit einer Größe von maximal ¼ Zoll oder 0,635 cm zerkleinert.
- CDs, DVDs, Sicherungsbänder, Audiokassetten und Videokassetten werden auf eine Größe von ½ Zoll oder 1,27 cm zerkleinert.
- Papierdokumente werden vor Ort geschreddert.

Standards für die Löschung von Festplatten

- Alle Festplatten, die zur Vernichtung oder Entsorgung bereitstehen, müssen mit dem DBAN-Dienstprogramm gelöscht werden.
- Löschmethode des US-Verteidigungsministeriums
- 7 Durchgänge
- Verifizierung aktivieren

Verfahren bei Datenpannen

Eine Datenpanne ist jeder Vorfall, bei dem die Vertraulichkeit, Integrität oder Verfügbarkeit von Ipsos-Informationsressourcen tatsächlich oder vermutlich verletzt wurde. Im Falle von Lieferanten bezieht sich dies auf die von Ipsos bereitgestellten Kundenstichproben.

Beispiele hierfür sind:

- Diebstahl oder Verlust eines Laptops, PCs, USB-Sticks, kleinen Computergeräts oder eines anderen Computer-/Speichergeräts, das von Ipsos bereitgestellte Kundenstichproben enthält.
- Vermuteter oder anderweitig bestätigter unbefugter Zugriff (Hack) auf das Netzwerk/die Hosts des Anbieters, auf denen von Ipsos bereitgestellte Kundenstichproben gespeichert sind.
- Erfolgreicher Virus-/Malware-Angriff auf ein System, das von Ipsos bereitgestellte Kundenstichproben enthält.

Für den Fall, dass von Ipsos bereitgestellte Kundenstichproben durch ein Verschulden des Anbieters ungewollt an die Öffentlichkeit gelangen, wird der Anbieter folgende Maßnahmen zur Reaktion auf den Vorfall ergreifen:

- Der Anbieter muss seinen Ansprechpartner bei Ipsos über die Verletzung informieren.
- Der Anbieter leitet unverzüglich eine Untersuchung der Datenpanne ein.

- Der Anbieter wird bei der Untersuchung mit Ipsos zusammenarbeiten und alle relevanten Systemprotokolle und Beweise unverzüglich an Ipsos weitergeben.
- Im Rahmen der Untersuchung wird eine Ursachenanalyse durchgeführt, um die Ursachen zu ermitteln und Empfehlungen zur Verbesserung der Informationssicherheit zu geben, damit sich solche Vorfälle in Zukunft nicht wiederholen.
- Eine Risikobewertung und empfohlene Gegenmaßnahmen werden in den Abschlussbericht aufgenommen.

Zugriffsverwaltung

Der Anbieter muss:

- sicherstellen, dass Kontrollen andere Kunden des Anbieters daran hindern, auf Ipsos-Assets zuzugreifen, es sei denn, dies wurde ausdrücklich schriftlich von Ipsos genehmigt.
- Verwenden Sie Authentifizierungs- und Autorisierungstechnologien für Konten auf Service-, Benutzer- und Administratorebene.
- Verhindern Sie, dass Mitarbeiter des Anbieters oder Unterauftragsverarbeiter direkten Root-Zugriff auf Systeme oder Zugriff auf das Administratorkonto eines Systems haben, das für die Bereitstellung von Dienstleistungen für Ipsos verwendet wird.
- Stellen Sie sicher, dass IT-Administratoren separate und eindeutige Administratorkonten erhalten und verwenden, die ausschließlich für Verwaltungsaufgaben genutzt werden. Nicht-Administrator-Aufgaben müssen immer mit Nicht-Administrator-Benutzerkonten ausgeführt werden.
- Stellen Sie sicher, dass für IT-Systeme, die auf Ipsos-Ressourcen zugreifen, Passwortrichtlinien und -standards existieren.
- Stellen Sie sicher, dass Systeme, die auf vertrauliche, personenbezogene oder regulierte Informationen zugreifen, jederzeit die folgenden Anforderungen an die Passwortkonstruktion erfüllen:
 - i. Mindestlänge von 8 Zeichen
 - ii. Komplexität: Mindestens drei der folgenden vier Zeichen müssen enthalten sein (Zahl, Großbuchstabe, Kleinbuchstabe, druckbares Sonderzeichen)
 - iii. Bei der Änderung oder Rotation eines Kontopassworts ist die Wiederverwendung eines der letzten 6 Passwörter nicht zulässig
 - iv. Das Ablaufdatum des Kontopassworts (die Anforderung, ein bestehendes Kontopasswort zu ändern) muss bei maximal 90 Tagen liegen.
 - v. Dienstkonten müssen nach spätestens 90 Tagen geändert werden.
 - vi. Bei mehr als 3 fehlgeschlagenen Anmeldeversuchen in Folge muss das Konto gesperrt werden.
 - vii. Bildschirmschoner-Sperren müssen aktiviert sein, um den Zugriff nach 30 Minuten Inaktivität des Benutzers zu sperren.

Der Anbieter muss sicherstellen, dass Systeme, die auf Ipsos-Assets und/oder das Ipsos-Netzwerk zugreifen, jederzeit die folgenden zusätzlichen Anforderungen erfüllen:

- i. Authentifizierungsdaten müssen bei der Speicherung oder Übertragung jederzeit verschlüsselt sein.
- ii. Passwörter für Benutzerkonten dürfen nicht von mehreren Personen gemeinsam genutzt werden.
- iii. Der Anbieter muss Passwörter sofort ändern, wenn der Verdacht besteht, dass ein Konto kompromittiert wurde.
- iv. Passwörter dürfen nicht per E-Mail oder anderen Formen der elektronischen Kommunikation weitergegeben werden, mit Ausnahme von Einmalpasswörtern.
- v. Passwörter für einzelne Benutzerkonten dürfen niemals an andere Personen als den Kontoinhaber weitergegeben oder mit diesen geteilt werden.
- vi. Die Identität eines Benutzers muss überprüft werden, bevor sein Passwort zurückgesetzt wird, und es muss eine E-Mail- oder Voicemail-Benachrichtigung gesendet werden, um den Benutzer darüber zu informieren, dass sein Passwort zurückgesetzt wurde.
- vii. Erstmalige Passwörter für neue Benutzerkonten müssen eindeutige Werte haben, die den Anforderungen dieser Richtlinie entsprechen, und dürfen keine generischen, leicht zu erratenden Passwörter sein.
- viii. Benutzerkonten müssen so konfiguriert werden, dass bei der ersten Verwendung eines neuen Kontos oder nach dem Zurücksetzen eines Passworts eine Änderung des Passworts erzwungen wird.
- ix. Alle Herstellerpasswörter müssen von ihren Standardwerten geändert werden (auch wenn der Standardwert NULL ist) und müssen den in dieser Richtlinie festgelegten Anforderungen entsprechen. Herstellerpasswörter umfassen unter anderem SNMP-Community-Strings und Passwörter für Administratorkonten auf Systemebene.
- x. Temporäre Kontopasswörter, drahtlose Verschlüsselungsschlüssel und andere Standard-Authentifizierungseinstellungen.
- xi. Passwortfelder dürfen, sofern technisch möglich, nur maskierte Zeichen anzeigen, während der Benutzer sein Passwort eingibt.
- xii. Hardcodierte Klartext-Passwörter dürfen in Produktionsumgebungen nicht verwendet werden.
- xiii. Produktionskontokennwörter dürfen nicht in Nicht-Produktionsumgebungen verwendet werden.
- xiv. Wenn ein Administratorkonto auf Systemebene (z. B. lokaler Windows-Administrator oder UNIX/Linux-Root) zur privilegierten Verwaltung eines Geräts verwendet wird, muss dieses Passwort nach Abschluss dieser Verwaltungsaufgabe geändert werden.
- xv. Wenn ein Konto über ein vom Computer festgelegtes komplexes Passwort mit mindestens 20 Zeichen verfügt, auf das keine Person Zugriff hat oder das keiner Person bekannt ist, muss dieses Passwort während seiner Lebensdauer nicht geändert werden, es sei denn, das Konto oder das zugehörige System steht unter Verdacht, kompromittiert worden zu sein.
- xvi. Passwörter für Konten auf Systemebene müssen auf jedem Gerät eindeutig sein.

xvii. Alle Systeme müssen Benutzer zur erneuten Authentifizierung auffordern, wenn sie versuchen, ihre Berechtigungen auf höhere Sicherheitsstufen zu erhöhen. *Beispiele hierfür sind die Verwendung von sudo oder su auf UNIX/LINUX-Systemen oder „Ausführen als“ für Microsoft Windows-basierte Systeme.*

- Der Anbieter muss sicherstellen, dass Verfahren für die sofortige Änderung oder Beendigung von Zugriffsrechten oder Berechtigungen als Reaktion auf organisatorische Änderungen vorhanden sind.
- Der Anbieter muss sicherstellen, dass Verfahren für die Bereitstellung privilegierter Konten vorhanden sind.
- Der Anbieter muss regelmäßig die Notwendigkeit privilegierter Zugriffskonten überprüfen.
- Wenn der Anbieter Fernzugriff auf Ipsos-Ressourcen benötigt, muss er stets eine von Ipsos genehmigte Methode verwenden, um eine Fernverbindung zu Ipsos-Ressourcen herzustellen.

Beschaffung, Entwicklung und Wartung von Informationstechnologie

Der Anbieter muss:

- sicherstellen, dass regelmäßige Bewertungen der Schwachstellen der Infrastruktur, des Netzwerks und der Anwendungen durchgeführt werden und branchenübliche Verfahren zum Schwachstellenmanagement befolgt werden
- sicherstellen, dass branchenübliche Sicherheitsstandards für die Anwendungsentwicklung eingehalten werden, damit IT-Systeme und Anwendungen in jeder Phase des Anwendungs- und Systementwicklungszyklus getestet und gesichert werden.
- sicherstellen, dass Software und Anwendungsquellcode vor der Bereitstellung in der Produktion auf Schwachstellen und Sicherheitslücken überprüft und getestet werden.

Management von Vorfällen im Bereich der Informationssicherheit

Der Anbieter muss:

- Sicherstellen, dass Verfahren zur Überwachung und Protokollierung von Zugriffen und Aktivitäten, einschließlich Zugriffsversuchen und privilegierten Zugriffen, vorhanden sind.
- Sicherstellen, dass die Protokollierung alle Protokolle von Einrichtungen, Anwendungen, Servern, Netzwerkgeräten und IDS/IPS umfasst, die zentral verwaltet und mindestens 12 Monate lang aufbewahrt werden.
- Sicherstellen, dass Verfahren zur Planung und Benachrichtigung bei Sicherheitsvorfällen vorhanden sind, um alle Vorfälle im Zusammenhang mit Ipsos-Vermögenswerten zu überwachen, darauf zu reagieren, sie zu melden und zu untersuchen.
- Ipsos unverzüglich benachrichtigen, wenn der Anbieter eine Verletzung von Kontrollen feststellt, die sich auf die für Ipsos erbrachten Dienstleistungen, Vermögenswerte von Ipsos oder Daten im Zusammenhang mit Vermögenswerten von Ipsos auswirkt.
- Hinweis: Sobald der Anbieter eine Sicherheitsverletzung entdeckt oder davon benachrichtigt wird, muss er diese untersuchen, beheben, wiederherstellen und eine Ursachenanalyse durchführen.
- Stellen Sie Ipsos die Ergebnisse und regelmäßige Statusaktualisierungen aller Untersuchungen im Zusammenhang mit Ipsos zur Verfügung.
- Der Anbieter muss die Mitarbeiter der globalen Informationssicherheit von Ipsos dauerhaft über das Ergebnis der Untersuchung informieren.

Outsourcing

Wenn eine Dienstleistung vom Anbieter ausgelagert wird, muss der Prozess von den zuständigen Mitarbeitern des Anbieters verwaltet werden und es muss ein Vertrag vorliegen, der alle Anforderungen von Ipsos an die Informationssicherheit abdeckt.

Beantragung einer Ausnahme von der Richtlinie

Anträge auf Ausnahmen von der Informationssicherheitsrichtlinie müssen vom Anbieter begründet und vom globalen Informationssicherheitspersonal schriftlich genehmigt werden.