Nutzungshinweise

Abacus Hosting und AbaWebTreuhand

Version	Datum	Kommentar
1.0	13.06.2018	Finale Version

Inhaltsverzeichnis

1 Einleitung

Nachfolgende Ausführungen gelten für Kunden (nachfolgend Auftraggeber), welche Abacus Hosting Standard/Private und Abacus AbaWebTreuhand der OBT AG nutzen. Der Auftraggeber ist dafür verantwortlich, dass er und weitere verantwortliche Personen diese Nutzungs- und Sicherheitshinweise gelesen und verstanden hat.

2 Allgemein

Durch den Datenverkehr mit externen Stellen können Bedrohungen für die IT-Infrastruktur der OBT AG und für die OBT AG selber entstehen. Neben dem Verlust der Vertraulichkeit, der Integrität sensitiver Informationen und der Verfügbarkeit der Informatikmittel kann das ganze IT-System Ziel von Angriffen von innen und aussen sein. Diesem Umstand ist mit einem verantwortungsvollen Umgang mit den von der OBT AG zur Verfügung gestellten Benutzerkonten und Abacus-Software Rechnung zu tragen.

3 Verantwortung

Der Auftraggeber ist selbst dafür verantwortlich, dass er bei der Benutzung des Hosting-Angebots nicht gegen die Rechtsordnung (z.B. Strafrecht, Datenschutz) verstösst bzw. die Rechte Dritter (z.B. Urheberrechte, Lizenzrechte, Persönlichkeitsrechte) verletzt. Dies bedeutet insbesondere folgendes:

- Der Auftraggeber trägt die Verantwortung für den verantwortungsvollen Umgang ihrer Mitarbeitenden mit den Abacus Hosting- und Abacus AbaWeb-Produkten
- Entdeckte oder vermutete Sicherheitsprobleme sind der OBT AG (support@obt.ch) umgehend mitzuteilen.

4 Abacus Hosting

4.1 Allgemeine Sicherheitsempfehlungen

- Prüfen Sie jeden externen elektronischen Datenträger vor Gebrauch auf Schadsoftware.
- Sperren Sie beim Verlassen des Arbeitsplatzes den Computer.
- Laden Sie nie vom Internet Dateien von einer unbekannten, nicht vertrauenswürdigen oder seltsamen Quelle herunter.
- Geben Sie nie individuelle Passwörter intern oder extern weiter.
- Notieren Sie keine Passwörter, ausser in dafür vorgesehenen Programmen.
- Ändern Sie Passwörter umgehend, wenn:
  - es Gruppenpasswörter sind und sich die Zusammensetzung der Gruppe ändert.
  - unautorisierte Personen Kenntnis davon haben.
  - es sich um Initialpasswörter für die erste Anmeldung handelt.

4.2 Nutzung und Abgrenzung von mobilen Lösungen

Die OBT AG möchte darauf hinweisen, dass bei der Nutzung von mobilen Lösungen auf Tablets und Smartphones ein erhöhtes Risiko von Verlust/Diebstahl besteht.

Obschon Produkte wie AbaCliK oder AbaSmart die Sicherheitsmechanismen der Betriebssysteme (iOS und Android) nutzen, besteht ein Restrisiko aufgrund der Tatsache, dass sich Informationen des Auftraggebers auf den mobilen Geräten gespeichert werden.

- Nutzen Sie wenn möglich als Bildschirmsperre eine PIN, ein Muster oder ein Kennwort und

aktivieren die zeitabhängige Gerätesperre (z.B. nach zwei Minuten). Entsperren Sie das Gerät nur unter Sichtschutz.

- Lassen Sie bei Verlust Ihres mobilen Gerätes die SIM-Karte unverzüglich sperren und die Datensynchronisation löschen.
- Achten Sie darauf, ob es Sicherheitsupdates für Ihr portables Gerät (Firmware, Betriebssystem) oder für von Ihnen installierte Apps gibt, und führen Sie diese durch.
- Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, sollten Sie vorher alle Datenspeicher löschen.

4.2.1 Verwendung von AbaCliK

Die Zugriffsberechtigungen für die Verwendung von AbaCliK wird innerhalb eines Abacus-Mandanten und nicht durch von der OBT AG betriebene Benutzerverwaltung gesteuert. Es steht dem Auftraggeber frei seine Mitarbeitenden für die Verwendung von AbaCliK freizugeben oder einzuschränken. Die korrekte Freigabe für die Nutzung von AbaCliK und auf Informationen innerhalb des Mandanten (z.B. Konten und Geschäftsbereiche) liegt somit in der Verantwortung des Kunden. Die OBT AG hat keinen Einfluss bezüglich Sicherheitsrisiken im Zusammenhang der Berechtigungsvergabe für AbaCliK.

Die OBT empfiehlt die Authentifizierung von AbaCliK per IDP (Identity Provider) wie SuisseID oder Mobile ID zu konfigurieren. Die OBT hat keinen Einfluss darauf, wie der Auftraggeber den Zugriff der Smartphone App konfiguriert.

Des Weiteren empfiehlt die OBT AG das Einrichten eines zusätzlichen Passwort- oder PIN-Schutzes für die Nutzung von AbaCliK.

Um die vollständige Funktionalität von AbaCliK zu nutzen, werden einige Informationen (Lizenzinformationen und fotografierte, hochgeladene Belege) nicht direkt in die von der OBT AG betriebene Abacus-Installation gespeichert, sondern in der von der Abacus Research AG betriebenen zentralen Plattform "AbaSky" verarbeitet und zwischengespeichert.

4.2.2 Verwendung von AbaSmart

Über die Tablet-App „AbaSmart“ lässt sich die Funktion „Ortungsdienst“ aktivieren. Die OBT AG empfiehlt die Deaktivierung des Ortungsdienstes innerhalb der App oder innerhalb des jeweiligen Betriebssystems. Wird die Funktion innerhalb der App durch den Benutzer aktiviert, so wird dessen Standort innerhalb der Abacus-Software zentral registriert. Sollten Benutzer die Funktion aktivieren, so unterlässt die OBT AG die aktive Verarbeitung, Auswertung oder Einsicht dieser Standortdaten, welche nicht im Sinne der betroffenen Person ist. Eine Verarbeitung und Nutzung der Standortdaten ausserhalb der Zweckbestimmung des jeweiligen Vertrages ist der OBT AG nicht gestattet.

Die OBT AG darf jedoch nach Rücksprache Arbeiten durchführen, die zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind (z. B. die Erstellung von Sicherheitskopien und die Durchführung von Migrationen im Rahmen technischer Weiterentwicklungen) sowie so mit den Daten umgehen, wie es im Hinblick auf die Einhaltung gesetzlicher Pflichten der Vertragspartner erforderlich ist.

4.2.3 Verwendung von MyAbacus

Der Zugriff auf MyAbacus erfolgt per Webbrowser und dem üblichen Abacus-Benutzerkonto. Die Zugriffsberechtigungen auf Informationen innerhalb eines Mandanten über MyAbacus wird im Mandanten selber und nicht durch die von der OBT AG betriebene Benutzerverwaltung gesteuert. Es steht dem Auftraggeber frei seine Mitarbeitenden für die Verwendung von MyAbacus freizugeben oder einzuschränken. Die korrekte Freigabe für die Nutzung von MyAbacus und auf Informationen innerhalb des Mandanten liegt somit in der Verantwortung des Kunden. Die OBT AG hat keinen Einfluss bezüglich Sicherheitsrisiken im Zusammenhang der Berechtigungsvergabe für MyAbacus.

4.2.4 Verwendung von AbaNinja

Der Zugriff auf AbaNinja erfolgt per Webbrowser und einem separaten Benutzerkonto. Die darin verarbeiteten Informationen befinden sich nicht in der von der OBT AG betriebenen Abacus-Installation, sondern in der von Abacus Research AG betriebenen und entwickelten Plattform.

Es steht dem Auftraggeber frei seine Mitarbeitenden für die Verwendung von AbaNinja freizugeben oder einzuschränken. Die korrekte Freigabe für die Nutzung von AbaNinja und auf Informationen innerhalb des Mandantenliegt somit in der Verantwortung des Kunden. Die OBT AG hat keinen Einfluss bezüglich Sicherheitsrisiken im Zusammenhang der Berechtigungsvergabe für AbaNinja.

4.3 Umgang mit unpersönlichen Benutzerkonten

Unpersönliche Benutzerkonten (z.B. Schalter- bzw. Kassenarbeitsplatz, Sitzungszimmer) sind aufgrund der möglichen Risiken bezüglich Daten- und Zugriffschutz sowie Nachvollziehbarkeit wenn immer möglich zu vermeiden. Falls aufgrund betriebsorganisatorischer Umstände unpersönliche Benutzerkonten verwendet werden, achten Sie auf folgende Massnahmen:

- Stellen Sie sicher, dass mittels unpersönlichen Benutzerkonten keine persönlichen bzw. datenschutzrelevanten Informationen verarbeitet oder gespeichert werden.
- Führen Sie ein Protokoll darüber, welcher Mitarbeitende zu welchem Zeitpunkt auf welche unpersönlichen Benutzerkonten Zugriff hatten.
- Stellen Sie sicher, dass bei personellen Änderungen (Rollenwechsel, Kündigung, Pensionierung usw.) Passwörter von unpersönlichen Benutzerkonten umgehend geändert werden, um den Zugriffschutz weiterhin sicherzustellen.
- Stellen Sie sicher, dass unpersönliche Benutzerkonten nur für den vorgesehenen Zweck verwendet werden können bzw. dürfen.

4.4 Zugriff auf Kundeninformationen im Supportfall

Zur optimalen technischen sowie fachlichen Unterstützung des Auftraggebers ist grundsätzlich vorgesehen auch ohne aktive Einsicht dessen auf Kundeninformationen innerhalb der Abacus-Mandaten zuzugreifen. Gehen Supportfälle über ein Anwendungsproblem eines Benutzers hinaus, so ist es der OBT AG vorbehalten in Absprache mit dem Auftraggeber die Unterstützungsarbeiten im Hintergrund durchzuführen. Dies gilt auch für den Zugriff des Softwareherstellers Abacus Research AG, welche die OBT AG in besonders komplexen Problemstellungen und Aufträgen unterstützt. Dieses Vorgehen hält Kosten und Aufwände auf Seiten der OBT AG und des Auftraggebers möglichst klein und ermöglicht eine effektive Behandlung aller Kunden- und Supportaufträge. Wünscht dies ein Auftraggeber nicht, so ist dies schriftlich und explizit bekanntzugeben und das Vorgehen in einem Supportfall individuell zu besprechen.