

Verteiler:

- a) Fachbereiche, Abteilungen, Referate und Stabsstellen in der senatorischen Behörde
Umwelt, Bau und Verkehr

nachrichtlich:

- b) S, SV-BV

Dienstanweisung Nr. 446

(Aufgabenbereich: 01 - Organisation, Allgemeines)

**Austausch von Daten mit externen Personen über sichere
Datenaustauschplattformen im Internet**

1. Vorbemerkungen

Verwaltungsprozesse werden zunehmend digital abgewickelt. Die hierbei anfallenden Daten müssen in manchen Fällen Personen oder Organisationen zur Verfügung gestellt werden, welche keinen Zugriff auf die Systeme der Verwaltung erhalten können.

Beispiele hierfür wäre die Bereitstellungen von

- Plänen oder Bildmaterial an Ingenieurbüros oder Agenturen,
- Dokumenten an Dritte, die einen höheren Schutzbedarf haben, als es das E-Mail System bietet.

Aktuell werden diese Daten über USB-Sticks, optische / magnetische Datenträger oder E-Mails ausgetauscht. Hierbei entstehen vielerlei Probleme. Erstens ist über E-Mail nur eine geringe Größe von Dateien zugelassen. Die Annahme von USB-Sticks von Dritten ist aus Sicherheitsgründen nicht erlaubt, da hier Schadsoftware mit übertragen werden kann. Gleiches gilt für optische / magnetische Datenträger. Der Datenaustausch über Lösungen wie EGVP oder verschlüsselte Dateianhänge in E-Mails gestaltet sich unpraktisch, da hierfür alle am Datenaustausch beteiligte Parteien bestimmte Software installiert haben müssen.

Eine sichere Datenaustauschlösung im Internet würde alle Anwendungsfälle abdecken und wäre über die in der Regel auf den Rechnern installierten Internet-Browsern zu nutzen.

Nachfolgend werden Regeln zur Nutzung einer Datenaustauschlösung für alle Mitarbeitende verbindlich geregelt.

2. Allgemeine Regelungen

Im Folgenden wird der Begriff „Software“ für Datenaustauschlösungen genutzt.

2.1 Die Nutzung der Software ist ausschließlich zu dienstlichen Zwecken bzw. zur Erledigung der dienstlichen Aufgaben gestattet.

2.2 Die private Nutzung ist verboten.

2.3 Die Software darf nicht zur alleinigen Ablage von Dokumenten genutzt werden, es dürfen nur Kopien abgelegt werden.

2.4 Die Software darf nicht für Backups von Dokumenten genutzt werden.

3. Datenschutz

3.1 Es dürfen nur Daten mit Schutzbedarf „normal“ übertragen werden.

3.2 Nachdem der Datentransfer beendet ist, müssen die Daten aus der Software entfernt werden.

3.3 Werden Dokumente bereitgestellt, muss der Zugriff für Dritte mit einem Passwortschutz versehen werden.

3.4 Der Speicherort von Dokumenten und das Passwort dürfen Externen nicht über ein und dasselbe Medium (z.B. E-Mail) mitgeteilt werden. Das Passwort kann z.B. über Telefon oder per Brief mitgeteilt werden.

3.5 Die Weitergabe von persönlichen Benutzerkennungen und sonstigen Authentisierungshilfsmitteln an andere Personen ist unzulässig.

3.6 Der Umgang mit Kennwörtern oder auch anderen Zugangsberechtigungsverfahren erfordert besondere Umsicht und Sorgfalt:

- Kennwörter sind nicht zu notieren und niemandem mitzuteilen.
- Kennwörter dürfen nicht leicht zu erraten sein.
- Kennwörter sollten immer große und kleine Buchstaben, Zahlen und Sonderzeichen beinhalten.
- Die Mindestpasswortlänge beträgt acht Zeichen

3.7 Die Übertragung der Daten auf dem Transportweg ist verschlüsselt

3.8 Die Daten auf dem Speichersystem im Rechenzentrum sind verschlüsselt

4. Ausschluss von weiteren Datenaustauschlösungen

4.1 Produkte von dritten wie „Dropbox“, „Google Drive“, usw. sind nicht zulässig.

4.2 Um Daten Externen zur Verfügung zu stellen, darf nur die im Anhang beschriebene Software genutzt werden (Fall: SUBV bietet Daten an).

4.3 Sollen Dokumente aus externen Lösungen *bezogen* werden ist jeweils abzuwägen wie vertrauensvoll die Quelle ist. Bestehen Unsicherheiten Fragen sie beim IuK-Management nach. (Fall: SUBV bezieht Daten von Dritten)

5. Administration und Betrieb

5.1 Die Administration der Benutzer wird durch das IuK-Management vorgenommen und diese können dort beantragt werden.

5.2 Für jeden Anwendungsfall wird ein eigener geschützter Bereich eingerichtet. Auf diesen haben nur bestimmte Personen Zugriff.

5.3 Wenn vorhanden, hat die Administration Zugriff auf das „Audit-Log“ um bei missbräuchlicher Nutzung einschreiten zu können. Hiervon wird ausschließlich bei begründetem Verdacht Gebrauch gemacht.

5.4 In Abteilung 1 wird ein kleines Kontingent von Lizenzen bereitgehalten um anfallende Aufgaben im Tagesgeschäft abzuwickeln. Sind darüber hinaus dauerhaft viele Lizenzen für die Fachbereiche nötig, muss die Finanzierung sichergestellt sein.

6. Konkrete Software und Funktionen

Die aktuell genutzte Software, sowie die möglichen und erlaubten Funktionen sind in Anhang 1 beschrieben.

7. Inkrafttreten

Diese Dienstanweisung tritt am 01.03.2019 in Kraft

Bremen, den 15.02.2019

Staatsrat
- Ronny Meyer -

Anlage/n:
Anhang 1: Produkt „dDataBox“ der Dataport AöR

Anhang 1:

A1.1: Funktionen der Software „dDataBox“

A1.1.1 Clients

1. Webbrowser

Standardmäßig erfolgt der Zugriff auf die Cloud über Webbrowser (Internet-Explorer oder Edge).

2. Windows-Software (Einbinden der Cloud als Netzlaufwerk)

In bestimmten Fällen kann die Einbindung als Netzlaufwerk im Windows-Explorer erfolgen (Poweruser).

3. Outlook-Add-In

Das Outlook Add-In erlaubt, Dateianhänge in E-Mails durch Links in die dDataBox zu ersetzen. Diese Funktion ist nur in bestimmten Fällen sinnvoll (Poweruser).

4. Apps für iOS und Android

Die Nutzung von Apps ist in der Regel nicht erforderlich, da von hier aus keine Verbindung zu den dienstlichen Daten im Verwaltungsnetz hergestellt werden kann.

Besteht die Anforderung zur Nutzung von Apps um z.B. Daten für eine Fachanwendung zu erfassen (z.B. Fotos), muss hierzu ein gesondertes Sicherheits- und Datenschutzkonzept vorgelegt werden.

A1.1.2 Erlaubte Funktionen

1. Freigabe von Dokumenten für Externe über das Internet
2. Freigabe von Ordnern zur Ermöglichung des „Hochladens“ von Dokumenten für Externe.
3. Anlegen von Unterordnern und Dokumenten

A1.2 Datenhaltung

1. Für jede Anforderung wird ein eigener, sicherer Speicherbereich angelegt.
2. Die Anzahl der Nutzenden und der benötigte Speicherplatz wird jeweils individuell bei der Beantragung begründet.

A1.3 Audit-Log

Im Audit-Log wird jede Aktion protokolliert

- Benutzeranmeldungen
- Hinzufügen von Dateien und Ordnern
- Download und Upload von Dateien
- Das Protokoll zeigt die letzten 100 Tage

A1.4 Dokumentation

Weitere Dokumentation der Cloud-Software befindet sich hier: <https://wiki.ddatabox.de>

A1.3 Support

Die Einrichtung von Nutzern und Ordnern erfolgt durch das IuK-Management.

Support für das Produkt dDataBox erfolgt durch Dataport, Tel.: 4444