IT Sicherheitskonzept

V1.1

Stand März 2019

1. Inhalt

2. Änderungshistorie

V1.0	Februar 2019	Neuauflage
V1.1	März 2019	Passwortbeispiel ergänzt

3. Allgemeines

Die Regeln des JCD IT Sicherheitskonzeptes stellen für Personen, die im Auftrag des JCD Daten verarbeiten, eine Arbeitsanweisung dar, die zwingend zu befolgen ist.

Auch der Jeep Club Deutschland e.V. (im weiteren abgekürzt JCD) kommt heutzutage ohne Datenverarbeitung nicht mehr aus. Dementsprechend ist der JCD gemäß DSGVO zur Ausweisung eines Datenverarbeitungsverzeichnisses verpflichtet in dem wiederum Hinweise zur Handhabung der Sicherheit verlangt sind.

Der Betrieb des JCD muss so organisiert werden, daß er auch trotz der häufigen Personal- und Zuständigkeitswechsel unabhängig von einzelnen Personen und deren Kompetenzen weiter aufrecht erhalten werden kann. Ein Eigenbetrieb jedweder IT Infrastruktur erscheint damit nicht ratsam.

Der Club betreibt grundsätzlich keine IT Infrastruktur. Der JCD bedient sich dazu zahlreicher aufeinander abgestimmter Dienstleister. Diese Dienstleister setzen State-of-the-art Security Methoden ein um einen Basisschutz zu gewährleisten. Die datenverarbeitenden Personen greifen auf diese Dienste mit Hilfe privater IT Geräte zu.

Alle datenverarbeitenden Personen sind gehalten die allgemein anerkannten Sicherheitsregeln im Umgang mit Daten zu beachten. Dies sind insbesondere:

- ✔ Starke Passwörter nutzen (Min. 8 Zeichen inkl. Groß-/Kleinschreibung, Ziffern und Sonderzeichen)
- ✔ Eine gängige Methode für merkbare, starke Passwörter ist die Nutzung eines ganzen Satzes inkl. Zahlen und Interpunktion. Von diesem Satz verwendet man als Passwort nur jeweils die Anfangsbuchstaben, Ziffern und Interpunktion.

  Beispiel: **M**ünchen **h**atte **2**018 **e**in **N**etz **v**on **8** **U**-Bahn **L**inien**, d**ie **i**ch **r**egelmäßig **n**utzte**!**

  Wird zu: Mh2eNv8UL,dirn!
- ✔ Passwörter regelmäßig wechseln.
- ✔ Passwörter nicht für mehrere Datensysteme verwenden.
- ✔ Updates und Patches zu Betriebssystem und Anwendungssoftware allzeit aktuell halten.
- ✔ Aktuelle Virenscanner einsetzen.
- ✔ Auftretende Unstimmigkeiten unverzüglich dem zuständigen IT Leiter melden.
- ✔ Passwörter nicht schriftlich notieren. Ausnahme: KeePass – Club Empfehlung (siehe 4.12)
- ✔ Accounts und Passwörter nicht weitergeben. Ist dies unumgänglich (z.B. von Admin an Anwender) so ist dies ausschließlich persönlich mündlich, oder über eine end-to-end verschlüsselte Verbindung durchzuführen. Beispiel: WhatsApp
- ✔ Kenntnisse, die aus der Verarbeitung der Daten resultieren, nicht ausserhalb des berechtigten Personenkreises weiter geben.

4. Spezifische Sicherheitshinweise

Über die allgemeinen Sicherheitshinweise hinaus sind folgende spezifische Sicherheitshinweise im Umgang mit den einzelnen Systemen / Aufgaben zu beachten:

4.1. Mitgliederverwaltung

Die Mitgliederdatei darf nur auf lokalen, nicht weiter zugänglichen Verzeichnissen, oder aber in der Clubeigenen verschlüsselten Cloud gespeichert werden.

4.2. Beitragsverwaltung

Die Datei darf analog zur Mitgliedsdatei ebenfalls nur unzugänglich lokal, oder verschlüsselt in der verschlüsselten Cloud abgelegt werden.

4.3. Administration der Website

… erfolgt über ein lokales plattformübergreifendes Websitemanagementsystem Namens RocketCake. Um eine verteilte Bearbeitung der Seiten zuzulassen ist es erforderlich die Projektdatein und die Inhaltsdateien zu sharen. Es handelt sich hierbei ausschließlich um öffentlich zugängliche Daten. Es besteht kein Schutzanspruch. Google Drive ist daher ausreichend.

Im Gegenzug bedeutet die Nutzung einer weitgehend offenen Synchronisationsplattform wie Google Drive, daß im Rahmen des Website Managements keine personenbezogenen Daten, oder andere Daten mit vertraulichem Charakter im Projektdrive abgelegt werden dürfen.

Weiter ist zu beachten, daß Google Drive Daten in USA gehostet werden. Server in den USA unterliegen nicht den Europäischen Sicherheitsstandards oder Vorgaben wie der DSGVO. Personenbezogene Daten oder andere Daten mit Geheimhaltungsanspruch dürfen daher hier generell nicht abgelegt werden.

4.4. Administration der e-mail

… erfolgt im vom Hoster zur Verfügung gestellten Webinterface. Die Mailboxen der verwalteten user dürfen nicht geöffnet werden. Die entsprechenden Passwörter sind nur in Absprache mit dem betroffenen User zurückzusetzen.

Ausnahme: Scheidet ein User aus der Domäne jeep-club.de aus, so kann die Mailbox geöffnet werden um ggf. geschäftsrelevante Daten zu identifizieren und vor Löschung zu sichern.

4.5. Administration des Forums

… erfolgt im administrativen Interface der gewählten Serversoftware phpBB. Administrativ berechtigte accounts sehen dazu neben dem Schnellwahlmenü zusätzliche Funktionen. Eine administrative Berechtigung kann nur von einem bisherigen administrativ berechtigten account vergeben werden.

Der Ur-account namens admin kann nur bei der Neueinrichtung des Serverdienstes vergeben werden.

Die Mitgliedschaft in der Gruppe JCD Mitglieder führt zu erweiterten sichtbaren Foren. Die Mitgliedschaft in der Gruppe ist regelmäßig mit der Mitgliederverwaltung anhand der registrierten e-mail Adresse abzugleichen.

4.6. Administration der Facebookgruppe

… erfolgt in Facebook. Administrative Rechte können von anderen Administratoren vergeben werden. Der erste Administrator ist der Gruppenowner. Er erlangt seinen Status durch anlegen der Gruppe.

4.7. Administration der Datenablage

Der Club nutzt als gemeinsame Ablage eine Synchronisations- und Versionierungslösung von Lucky Cloud. Ein lokales Verzeichnis wird vom Seafile Client automatisch mit der ClubCloud synchronisiert. Dabei wird in der Übertragung eine TLS-Verschlüsselung eingesetzt. Zusätzlich nutzt der Club die angebotene End-to-end Verschlüsselung. Die Daten sind damit doppelt gesichert geschützt. Der Dienstleister und auch kein anderer dritter erhält keinen Einblick in die Daten.

Die betroffenen Server stehen in Deutschland bei einem deutschen Hoster und unterliegen damit deutschem Recht.

LuckyCloud wendet auf die Daten gleichzeitig eine Versionierung an. Damit besteht ein implizites Backup. Selbst im Falle einer irrtümlichen Löschung können Daten aus dem Papierkorb im Webclient restauriert werden.

Darüber hinaus ergibt sich ein weiteres Backup durch die Synchronisation auf alle teilnehmenden Rechner der Gruppe. D.h. jedes verarbeitende Mitglied der berechtigten Gruppe verfügt nochmal über lokale Kopien.

4.8. Administration der Vereinssoftware

Beschreibung wird nach Einführung (geplant März 2019) nachgereicht.

4.9. Betrieb des Fototauschdienstes

Der Fototauschdienst wird vom Mitglied Robert Brummer in privater Eigenleistung unentgeltlich erbracht. Es werden keine personenbezogenen Daten verarbeitet, ausser den von den Teilnehmern eines Events freiwillig zur Verfügung gestellten Fotografien. Alle Teilnehmer werden in der Eventanmeldung auf die Abtretung des Persönlichkeitsrechtes am Bild hingewiesen.

Die Teilnahme am Fototauschdienst bedarf einer Einladung die vom Betreiber anhand der Teilnehmerlisten (nur e-mails) verschickt wird. In der Einladung und auch in der Beschreibung auf dem Server wird u.a. darauf hingewiesen, daß nur Bilder hochgeladen werden dürfen zu denen der hochladende die Bildrechte besitzt.

Der Hochladende erklärt mit der Nutzung des Dienstes seine Abtretung der Bildrechte an den Club zu den im Anschreiben genannten Zwecken.

Ein Backup ist nicht erforderlich, da die Bilder keine kritischen Daten darstellen.

4.10. Geschäftsstelle

Die Geschäftsstelle dient dem JCD als zentrale Anlaufstelle für Post und e-mail. Die Geschäftsstelle dispatcht die eingehende Post auf die jeweils zuständigen organisatorischen Einheiten. Im Zweifelsfall werden Vorgänge dem Vorstand zur Entscheidung vorgelegt.

Eventanmeldungen werden erfasst und an Kassenwart und Eventleiter weiter gegeben.

Ausgehend verschickt die Geschäftsstelle Geburtstagsgrußkarten.

Die Geschäftsstelle nutzt zur Durchführung ihrer Aufgaben die Daten der Mitgliederverwaltung, damit auch personenbezogene Daten. Die Absicherung dieser Daten erfolgt mittels der allgemeinen Sicherheitshinweise und den hier dokumentierten spezifischen Hinweisen zu den verwendeten Systemen. Eine weitergehende Absicherung ist nicht erforderlich.

Der Vorstand ist dafür verantwortlich, daß der den in der Geschäftsstelle arbeitenden Personen die Regeln des JCD IT Sicherheitskonzeptes bekannt gemacht werden und diese eingehalten werden.

4.11. Eventbüro

Im Rahmen des Eventbüros werden die Teilnehmer eines Events gemanaged.

- Startnummern werden vergeben,
- Startgebührenzahlungen verifiziert und ggf. noch entgegen genommen,
- erforderliche Unterschriften unter Anmeldung und Haftungsausschluss von Fahrer und Beifahrer werden erfasst,
- Angaben zum Fahrzeug werden erfasst um daraus im Event eine passende Fahrzeugklasse und/oder einen sogenannten Handycapfaktor bestimmen zu können.

Dazu werden u.a. auch personenbezogene Daten erfasst und verarbeitet. Es sind jedoch keine spezifischen Sicherheitsanforderungen über die allgemeinen Hinweise hinaus erforderlich.

Der zuständige Eventleiter ist dafür verantwortlich, daß Orga, die für das Eventbüro eingeteilt wurde auch Kenntnis von den hier angesprochenen allgemeinen IT Sicherheitsregeln erlangt und diese auch beachtet.

4.12. Passwortsafes - Keepass

Dieser Abschnitt stellt eine Handlungsempfehlung dar, keine Arbeitsanweisung.

Angesichts zahlreicher unterschiedlicher IT Systeme, die alle ihr individuelles Login benötigen fragen sich Anwender wie man sich das alles merken soll. In der Tat gibt es zu diesem Thema eine eigene Software Kategorie, die dieses Problem weitgehend löst, die sogenannten Passwortsafes.

Ein Passwortsafe ist nichts weiter als eine kleine Tabelle von accounts und Passwörtern, die verschlüsselt gespeichert werden. Die Verschlüsselung erfolgt anhand eines sogenannten Masterpasswortes. Der User muss sich dann nur noch dieses eine Masterpasswort merken, alle anderen Daten sind innerhalb des Safes zugänglich.

Dieses Masterpasswort ist zwingend hochsicher zu wählen (siehe Passwort regeln im allgemeinen Teil). Es darf unter keinen Umständen in falsche Hände geraten, denn damit wäre nicht nur ein System kompromitiert, sondern alle Systeme des Users.

Vergisst der User das Masterpasswort, so ist es nicht möglich dieses zu rekonstruieren. Der Inhalt des Safes ist dann unwiederbringlich verloren.

Bei Nutzung eines solchen Passwortsafes kommt es maßgeblich darauf an, daß der Verschlüsselung des Hersteller vertraut werden kann. Hätte dieser z.B. eine Hintertür eingebaut, so könnte er spielend leicht alle accounts jedes users öffnen.

Unter internationalen Spezialisten gelten Open Source Systeme grundsätzlich als am sichersten, weil weltweit alle Spezialisten den Code des Programmes einsehen können. Hintertüren lassen sich so nicht verbergen und Fehler werden in kürzest möglicher Zeit gefunden und eliminiert.

Keepass ist ein solcher international anerkannter Open Source Passwortsafe. Und Keepass ist nicht nur Open Source (und damit kostenlos), es steht auch noch auf zahlreichen Plattformen zur Verfügung. Legt man also die Schlüsseldatei so ab, daß alle verwendeten Geräte darauf zugreifen können, dann hat man immer jederzeit an allen Geräten seine Passwörter aktuell zur Verfügung. In einem Moment arbeitet man noch an seinem PC, im nächsten Moment ist man mit dem Handy unterwegs, aber immer stehen die Passwörter zur Verfügung.

Eine solche gemeinsame Ablage kann durch Cloudsynchronisationsdienste erreicht werden, wie z.B. DropBox, Google Drive, OneDrive, Amazon Cloud Drive, MagentaCLOUD, iCloud oder auch selbst gebaute Lösungen sicher verschlüsselt wiederum über Open Source Software auf Basis des Seafile Clients.

Besonderes Features bei Keepass:

Zusätzlich zum Masterpasswort kann man auch noch eine Schlüsseldatei zur Verschlüsselung heranziehen. Mit dieser sogenannten Zwei-Faktor-Authentisierung wird das erreichte hohe Sicherheitsniveau nochmal mehr als verdoppelt. Freilich muss dann diese Schlüsseldatei auf allen Geräten gleichermaßen zur Verfügung gestellt werden und zwar auf einem anderen Verteilweg als dem Clouddrive. Also z.B. einmalig bei der Installation via USB Stick, oder schlimmstenfalls per WhatsApp (da WhatsApp mit seiner End-to-end Verschlüsselung wiederum einen gesicherten Übertragungskanal darstellt.

Keepass Clients können auf Geräten mit biometrischen Scannern diese anstelle des Masterpasswortes zur Öffnung nutzen. Damit kann man z.B. auf dem Handy per Fingerabdruck die Datei öffnen, ohne das Masterpasswort eingeben zu müssen – sehr praktisch.

Achtung: Bei Verwendung von biometrischen Scannern wird das Masterpasswort im betriebssystemeigenen, verschlüsselten Schlüsselbund abgelegt. Damit sinkt die Sicherheit des Gesamtsystems. Es ist deshalb in diesem Fall unerlässlich die Sicherheit durch Verwendung der oben erläuterten Zwei-Faktor-Authentisierung wieder auf ein hohes Niveau zu heben.

5. Umgang mit Dienstleistern

5.1. Allgemeines

Als Dienstleister im Sinne dieses IT Sicherheitskonzeptes werden Firmen verstanden, die regelmäßig personenbezogene Daten des JCD verarbeiten.

Dienstleister sind per Vertrag zu beauftragen. Darin ist die Art der Dienstleistung und die dafür erforderlichen Daten zu beschreiben. Es gilt das need to know Prinzip, d.h. es werden dem Dienstleister nur die Daten zur Verfügung gestellt, die für die Ausführung seiner Tätigkeiten erforderlich sind.

Der Dienstleister muss zusagen die Daten vertraulich zu behandeln. Die Daten des JCD dürfen vom Dienstleister auch nicht zum Zwecke der Eigenwerbung oder anderen Zwecken ausserhalb des Dienstleistungsvertrages eingesetzt werden.

Die Weitergabe der Daten an Dritte ohne schriftliche Zustimmung des JCD ist untersagt.

Dienstleister müssen die Daten in Deutschland auf in Deutschland stehenden Systemen verarbeiten, um zu gewährleisten, daß die Datenverarbeitungskette geschlossen deutschem Recht unterliegt.

Dienstleister müssen damit auch die Vorgaben der DSGVO einhalten.

Mit jedem Dienstleister ist eine DSGVO konforme Auftragsvereinbarung (AV) abzuschließen. Von größeren Dienstleistern liegen generische AVs vor. Diese können genutzt werden.

Neben den hier genannten Sicherheitsanforderungen sind selbstredend auch die einschlägigen deutschen Gesetze, wie z.B. Werksverträge und AÜG einzuhalten.

Ein Vertrag mit einem Dienstleister muss gemäß DSGVO die folgenden Inhalte regeln:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung

- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Liegt keine generische AV seitens des Dienstleisters vor, so ist die JCD Auftragsvereinbarung anzupassen und zu vereinbaren.

Die AVs sind vertraulich zu behandeln. Sie sind in der Club Cloud zu speichern und auf Anfrage berechtigten Personen auszuhändigen (z.B. Dienstleister, Prüfer Landesamt für Datenschutz, Datenschutzbeaufragte, usw.).

5.2. Twooit

AV liegt vor, siehe Datei „TwooIT AV-Vertrag.pdf“, oder Alternativ Download im Kundenportal von TwooIT unter https://ssl.twooit.com/

5.3. Facebook

Keine Verarbeitung von Clubdaten, da Facebook eine eigene Userverwaltung beinhaltet. Lediglich bei der Administration der Facebookgruppe werden temporär (Mitgliedsstatusabgleich) JCD Daten verwendet, aber nicht an Facebook übermittelt. Diese Verwendung erfolgt ausschließlich von einem JCD Mitglied, dem Administrator der Facebookgruppe (siehe JCD Datenverarbeitungsverzeichnis publiziert auf der JCD Website https://www.jeep-club.de).
Eine AV ist dementsprechend nicht erforderlich und liegt nicht vor.

5.4. Luckycloud

AV liegt vor, siehe Datei „luckycloud AV-Vertrag.pdf“.
(Status 13.2.2019: luckycloud stellt in wenigen Tagen ein Tool zur individuellen Generierung der AV zur Verfügung. Dann erfolgt download und Ablage)

5.5. Google

Google Drive wird ausschließlich zur gemeinsamen Nutzung der Website Projektdaten genutzt (siehe Administration Website). Es werden keine personenbezogenen Daten abgelegt. Die hier im Einsatz befindlichen Daten sind alle öffentlich einsehbar und Unterliegen keinerlei Geheimhaltung.
Eine AV ist dementsprechend nicht erforderlich und liegt nicht vor.

5.6. Claudia Kiesel

AV wird in Kürze abgeschlossen, künftig siehe Datei „Claudia Kiesel AV-Vertrag.pdf“.

5.7. NetXP

AV wird nach Vertragsabschluss zur Verfügung gestellt.