IT-Richtlinie

Dokumenteninformationen			
Klassifikation:	intern		
Versionsnummer:	2.1		
Dokumententitel:	IT-Richtlinie		
Dokumentenverantwortlicher:	Marvin Schmidtmer		
Erstellt am:	18.06.2018	Erstellt von:	Marvin Schmidtmer
		Funktion des Erstellers:	ISO
Letzte Überarbeitung:	27.01.2021	Nächste Überarbeitung:	10.01.2021
Freigabe am:	29.01.2021	Freigabe von:	Marius Jäger

Versionsverlauf			
Datum	Version	Beschreibung	verändert durch
05.05.2020	2.0	Anpassung an CI, Versionierung eingefügt, Anpassung an Stand der Technik	Marvin Schmidtmer, Christian Nolle, Isabel Müller-Wilckens
07.12.2020	2.1	„Unternehmen“ durch „Jäger Group“ ersetzt, formelle Anpassungen	Marvin Schmidtmer
27.01.2021	2.1	Anpassung Kapitel 9.	Marvin Schmidtmer

Mitgeltende Dokumente:

1. Einleitung

Die IT-Richtlinie unterstützt die von der Jäger Group getroffenen Maßnahmen zum Schutz von (betriebsinternen und personenbezogenen) Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeiter und ist darüber hinaus eine verbindliche Richtlinie für alle Mitarbeiter im Hinblick auf den Umgang mit diesen Daten.

2. Geltungsbereich

Die IT-Richtlinie gilt für alle Mitarbeiter/innen der Jäger Group. Dazu gehören alle Festangestellten, Teilzeitangestellte, Auszubildende, Werkstudenten sowie Aushilfskräfte, Praktikanten etc. Die Jäger Group wird jeweils entsprechende Vorkehrungen treffen, damit diese IT- Richtlinie auch für externe Personen bzw. Dienstleister verbindlichen Charakter hat, sofern diese die Kommunikationsmittel/IT-Systeme der Jäger Group bearbeiten und von den Daten Kenntnis erlangen.

3. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen der Jäger Group sind von den Mitarbeitern die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Die Jäger Group informiert die betreffenden Mitarbeiter zeitnah über ihre rechtlichen Verpflichtungen durch eine entsprechende Schulung.

4. Allgemeine Regelungen

Die Nutzung der IT-Systeme und Applikationen in der Jäger Group sind ausschließlich zu dienstlichen Zwecken und in jeweils erlaubtem Umfang zur Erledigung der vereinbarten Tätigkeit zulässig. Abweichungen hiervon bedürfen der ausdrücklichen Zustimmung des Arbeitgebers, die schriftlich oder in Textform erfolgen muss.

Die Installation von Software zu privaten Zwecken ist untersagt. Im Übrigen darf nur Software auf IT-Systemen der Jäger Group installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.

Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ohne Zustimmung des Arbeitgebers schriftlich oder in Textform ist nicht zulässig. Die dienstliche Nutzung von USB Speichermedien ist nur nach Freigabe und Ausgabe durch die IT-Abteilung erlaubt. Im privaten Umfeld ist die Nutzung dienstlicher USB Speichermedien (z.B. USB-Sticks, SD-Karten, etc.) nicht gestattet.

5. Nutzung von Smartphones und Tablets

Die Jäger Group verwendet Software zur Verwaltung von mobilen Geräten. Dadurch wird die geschäftliche Nutzung auf dem Gerät isoliert und der Datenaustausch mit anderen Apps verhindert. Im Verlustfall und unter Abwägung der Verhältnismäßigkeit kann die Software dazu genutzt werden das Smartphone oder Tablet zu orten. Im Falle eines Verlustes besteht die Möglichkeit das Gerät aus der Ferne zu sperren/löschen. Die Ortung im Verlustfall darf nicht zu arbeitsrechtlichen Konsequenzen für den Mitarbeiter führen.
Zur Nutzung der App Stores darf nur die geschäftliche Emailadresse verwendet werden. Die private Nutzung der im Rahmen von Flatrates abgedeckten Dienste auf dienstlichen Smartphones ist erlaubt.
Das Anlegen und Speichern von geschäftlichen Kontakten in der lokalen Kontakte App/ im Adressbuch ist untersagt.

6. Cloud Dienste

Clouddienste umfassen sowohl Anwendungen, die nicht mehr im Jäger Rechenzentrum installiert sind, als auch jegliche Drittanbietersoftware, die das Speichern von Daten in der öffentlichen Cloud ermöglicht.
Die Nutzung von Drittanbietersoftware in der Cloud, die nicht durch die IT freigegeben wurde, ist untersagt.
Die Jäger Group prüft jeden Datenverkehr im Unternehmensnetzwerk. Sollte es zur unrechtmäßigen Nutzung von Clouddiensten durch einen Mitarbeiter kommen, behält sich die Jäger Group vor arbeitsrechtliche Schritte einzuleiten.

7. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu betriebsinternen oder personenbezogenen Daten erhalten, ohne hierfür berechtigt zu sein. Beim Verlassen des Arbeitsplatz-PCs ist der jeweilige Mitarbeiter verpflichtet das elektronische Arbeitsmittel zu sperren, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme
– so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird.

Jegliche Betriebsvorgänge/-informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

8. Passwortgebrauch

Soweit technisch möglich, sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers zu bedienen. Die Authentifizierung erfolgt durch die Verwendung der Kombination Benutzername/Passwort. Die IT- Abteilung wird, soweit keine betrieblichen oder technischen Gründe entgegenstehen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen.
Passwörter müssen eine Mindestlänge von 10 Zeichen haben. Das Passwort muss 3 von 4 Zeichenarten enthalten (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen). Zeichenketten, eigene Namen und allseits bekannte Passwörter sind nicht erlaubt (z.B. 123456aaaa, P@ssw0rd, etc.). Die Passwörter sind so zu wählen, dass Dritte nicht ohne größere Anstrengungen hiervon Kenntnis erlangen können. Bereits genutzte Passwörter können nicht erneut verwendet werden.
Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initialpasswort unverzüglich zu ändern.

Die Weitergabe des eigenen Passwortes an andere Mitarbeiter ist untersagt. Die Jäger Group behält sich vor, bei Verstoß arbeitsrechtliche Schritte einzuleiten.

9. Schutz vor Schadinhalten (Malware), Phishing und SPAM

Zum Schutz vor Schadinhalten werden in der Jäger Group Virenschutzprogramme und Firewalls eingesetzt. Der Datenverkehr im Netzwerk wird kontinuierlich auf schädliche Verhaltensmuster überprüft. Dabei kann es passieren, dass Verbindungen geblockt werden. Die E-Mail-Kommunikation wird zum Schutz vor Schadsoftware, Phishing und Spam u.a. durch Advanced Malware Protection (AMP) und Spamfilter überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Die Löschung wird durch eine Benachrichtigungs-Email ersichtlich.

Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist dieser verpflichtet, sich unverzüglich an den Information Security Officer oder die IT Abteilung zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch den Information Security Officer oder die IT Abteilung geöffnet werden.

Benutzer erhalten eine Benachrichtigung per E-Mail von quarantine@messaging.microsoft.com, sobald sich eine Nachricht für sie in der Quarantäne befindet. Sie erhalten die Möglichkeit den Absender dauerhaft zu blocken, die E-Mail an das eigene Postfach freizugeben oder die E-Mail zu überprüfen. Herrscht Unsicherheit darüber, ob die E-Mail unschädlich ist, sollte sie vor der Freigabe immer vom Verantwortlichen für IT-Sicherheit überprüft werden.

10. Nutzung von E-Mail/Internet/Festnetztelefon

Die Nutzung von E-Mail, Internet und Festnetztelefon darf nur für dienstliche Zwecke erfolgen. Es gelten die im Folgenden beschriebenen Ausnahmen.

Den Mitarbeitern ist es gestattet, private E-Mails über ihren eigenen, privaten Webmail-Account im Internetbrowser zu empfangen und zu senden. Der Umfang dieser Nutzung kann aus betrieblichen

Gründen von der Jäger Group eingeschränkt werden. Die private Nutzung des Internets wird in den Pausenzeiten geduldet, dies kann aber auch in Einzelfällen jederzeit widerrufen werden.

Generell unzulässig ist das Aufrufen von Webseiten, das Zugreifen auf oder Verteilen von Material, sofern eine derartige Handlung rechtswidrig ist oder von anderen Personen als geschmacklos, Anstoß erregend oder respektlos angesehen werden könnte.

Beispiele hierfür sind:
-Material, das sexuell eindeutige Bilder und Beschreibungen enthält,
-Material, das illegale Aktionen befürwortet,
-Material, das Intoleranz gegen Andere befürwortet.

Generell unzulässig ist aus Gründen der Datensicherheit auch die Verwendung der Firmen - UserID (E-Mailadresse und Anmeldename) zu privaten Zwecken im Internet.

11. Nutzung von WLAN

Die Nutzung des WLANs mit der Bezeichnung jaeger-WLAN ist mit dienstlichen Geräten erlaubt. Private Tätigkeiten z.B. das Schauen von Videos über Streamingdienste im WLAN sind weitestgehend zu unterlassen. Gäste erhalten generell keinen Zugang zum internen WLAN. Hierfür steht ein Gastzugang mit der Bezeichnung jaeger-Guest zur Verfügung. Freischaltungen sind am Frontoffice erhältlich.
Das WLAN am Laptop muss ausgeschaltet werden, wenn das Gerät am Arbeitsplatz angeschlossen und per LAN-Kabel verbunden ist.
Auch für die Nutzung des Internets über WLAN gelten die Bestimmungen zur Internetnutzung gemäß Punkt 10 dieser Richtlinie.

12. Verhalten bei Sicherheitsvorfällen

Sollte der Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, ist dies unverzüglich an den Information Security Officer zu melden und der Vorgesetzte sowie die Datenschutzbeauftragte zu informieren.