Stand: 2019-09-10

Nutzungsbedingungen der Dienste und konfigurierten Anwendungen des Verfahrens WiBeS

(Stand: 10.09.2019)

Inhalt

Ronald Wiegand

1 Geltungsbereich dieser allgemeinen Nutzungsbedingungen

Das Wissensmanagement für Berufliche Schulen (WiBeS) des Hamburger Instituts für Berufliche Bildung (HIBB), einem Landesbetrieb der Behörde für Schule und Berufsbildung (BSB), stellt die angebotenen Dienste und konfigurierten Anwendungen auf der Grundlage der nachfolgenden allgemeinen Nutzungsbedingungen zur Verfügung. Die Plattform wird technisch von Dataport AöR im Schutzbedarf „HOCH“ nach BSI[1] in einem Rechenzentrum betrieben. WiBeS behält sich das Recht vor, diese Nutzungsbedingungen für die Zukunft zu ändern oder zu ergänzen.

Die Nutzung der Dienste und konfigurierten Anwendungen, die durch WiBeS bereitgestellt werden (Microsoft SharePoint, Microsoft Exchange, Passwort-Service, Learning-Management-System), erfolgt grundsätzlich freiwillig. Es gelten hierzu die einschlägigen Bestimmungen der EU-DSGVO[2],des Hamburgischen Datenschutzgesetzes[3], Hamburgischen Schulgesetzes[4], Schul- Datenschutzverordnung[5], § 94 Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Gouvernement und deren Anlagen (Allgemeine Regeln der Bürokommunikation); speziell Ziffer 9: Private Nutzung und die Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten (PC-RL) vom 01.06.2005 (IT-Handbuch; MittVw Seite 74).

2 Leistungsbeschreibung

Mit WiBeS gewährt das HIBB den Nutzerinnen und Nutzern[6] den Zugang zu einer Vielzahl von Diensten und konfigurierten Anwendungen, einschließlich zahlreicher Kommunikationsmittel, die Microsoft-SharePoint zur Verfügung stellt. Die Serviceleistungen werden in der jeweils von WiBeS in Abstimmung mit den zuständigen Stellen (fachlichen Leitstelle) als sachgerecht eingestuften Konfiguration und Gestaltung sowie mit dem Vorbehalt der Verfügbarkeit angeboten. Die Nutzung von WiBeS erfolgt für jede Dienststelle nach den Richtlinien des Betriebs- und Rechtekonzepts[7]. Darüber hinaus werden die Nutzungsbedingungen hinsichtlich mitbestimmungsrelevanter Tatbestände in einer Dienstvereinbarung zwischen dem HIBB und dem Gesamtpersonalrat (GPR) der BSB geregelt.

WiBeS gewährt seinen Nutzern u.a. die Möglichkeit zur Nutzung der folgenden webbasierten Funktionen und Serviceleistungen:

- E-Mail-Service (Microsoft Exchange) mit “Outlook Anywhere-” (Client-Outlook- Verknüpfung) und ActiveSync-Funktionalität (mobile Zugriffe) für autorisierte Anwender.

[1] BSI = Bundesamt für Sicherheit in der Informationstechnik.

[2] https://dsgvo-gesetz.de/

[3] § 5 HmbDSG

[4] § 98 und § 28 Absatz 1-6 HmbSG (Rechte und Pflichten aus dem Schulverhältnis)

[5] § 1 ff. SchulDSV HA 2006

[6] Es wird zur Vereinfachung und Lesbarkeit des Textes jeweils die maskuline Form benutzt.

[7] Bestandteil der Verfahrensbeschreibung nach § 9 HmbDSG bzw. der Dienstvereinbarung HIBB./.GPR

- Dienste und konfigurierte Anwendungen auf einer Microsoft SharePoint-Plattform.
- Passwort-Service (PWS) Dienste und konfigurierte Anwendungen auf einer Learning-Management-Plattform (LMS).
- Beratung und Unterstützung durch das WiBeS-Team des HIBB.

3 Registrierung

Zur Registrierung bei WiBeS müssen die Nutzer wahrheitsgemäße, genaue und aktuelle Angaben zur Person machen und diese Registrierungsdaten ggf. aktualisieren. Der Zugang zu WiBeS ist nur authentifizierten Benutzern möglich. Jeder Benutzer erhält einen Benutzer-Account, für den er selbst verantwortlich ist.

4 Passwort-Service (PWS)

Der Nutzer kann am PWS teilnehmen. Dazu muss er eine alternative E-Mail-Adresse als die WiBeS-E-Mail-Adresse in WiBeS hinterlegen, über die er im Bedarfsfall kontaktiert wird. Das alternative E-Mail-Postfach ist so zu schützen, dass eine nicht autorisierte Person Zugang zu diesem Postfach erhält. Postfächer, die von mehreren Personen benutzt werden, dürfen nicht verwendet werden.

5 Datenschutzhinweise

Alle Informationen zum Datenschutz finden Sie in den Datenschutzbestimmungen auf der WiBeS Portalstartseite (siehe Kachel unter „Navigation WiBeS“). Diese Informationen sind kein Bestandteil der Nutzungsbedingungen und bedürfen daher keiner formalen Einwilligung, sondern dienen nur zu Ihrer Information.

6 Zugriff auf Datenbestände und Inhalte

Für die auf der WiBeS-Plattform für Mitarbeiter zugänglichen Inhalte sind die jeweiligen Dienststellen-Leitungen verantwortlich.

Die Dienststellenleitung sorgt dafür, dass die geltenden Copyright-Bestimmungen (Urheberrechtsbestimmungen), das Betriebs- und Rechtekonzept[8] sowie vereinbarten Arbeitsweisen mit WiBeS und die Datenschutzbestimmungen (EU-DSGVO/Hamburger Datenschutz) eingehalten werden. Dazu bedient sie sich der Hilfe der jeweiligen WiBeS-Betreuer. Maßgeblich für den Umfang des Zugriffsrechts (Vollzugriff, Teilnehmen- und Leserechte) auf die WiBeS-Plattform ist die Befähigung, damit zu arbeiten und der durch WiBeS bewertete Arbeitszusammenhang hinsichtlich des Gesamtverfahrens.

[8] Bestandteil der Verfahrensbeschreibung nach § 9 HmbDSG bzw. der Rahmendienstvereinbarung HIBB./.GPR

Für die Umsetzung des Rechtekonzepts ist eine entsprechend geschulte und autorisierte Person (=„WiBeS-Betreuer“) verantwortlich. Die WiBeS-Betreuer werden dabei von WiBeS beraten und unterstützt. Vollzugriffsrechte erhalten grundsätzlich nur autorisierte Personen, die erfolgreich an einer administrativen WiBeS Benutzerrechte-Schulung teilgenommen haben.

Dies bedeutet, dass verantwortliche Funktionen (bspw. Leitungsmitglieder) und Zugriffsrechte nicht automatisch identisch sein müssen. Bei etwaigen Verstößen ist die fachliche Leitstelle durch die Dienststelle zu verständigen. Das gilt auch bei datenschutzrechtlichen Verstößen. Weitere Hinweise zu „Data Breach“ finden Sie in den Datenschutzbestimmungen. Der zeitlich befristete Zugriff von externen Personen (bspw. Schulinspektion, QM-Audits) auf spezifizierte Inhalte der Plattform wird nur über eine von der Dienststellen-Leitung oder durch sie autorisierte Person(en) bei WiBeS beauftragt.

WiBeS wird dienstlich genutzt. Die für die Verwendung von WiBeS einschlägigen Vorschriften sind in der Dienstvereinbarung und deren Anlagen festgelegt.

Auf die persönlichen Inhalte (Inhalte der MySite sowie Inhalte des E-Mail-Postfachs) hat grundsätzlich allein der Nutzer Zugriff. In begründeten Ausnahmenfällen kann in Anlehnung an die Vereinbarung nach § 94 HmbPersVG (Richtlinie für Bürokommunikation) ein Zugriff durch die Dienststelle erforderlich werden. Für Inhalte im Zusammenhang mit Teamarbeit oder anderen gemeinschaftlichen Arbeitszusammenhängen der Dienststelle ist derjenige Personenkreis (Gruppen) verantwortlich, für den nach dem geltendem Berechtigungskonzept entsprechende Zugriffsrechte eingerichtet sind.

Um eine reibungslose fachliche und technische Unterstützung für alle Dienststellen zu gewährleisten, haben die Mitarbeiter des WiBeS-Teams im HIBB sowie bei Ticketbearbeitungen und im Rahmen von Wartungsfenstern der Plattform auch Dataport-Administratoren Zugriff auf alle Inhalte der Dienststellen. Die betreffenden Personen sind namentlich benannt, zu besonderer Verschwiegenheit verpflichtet und greifen ausschließlich anlassbezogen auf die jeweiligen Bereiche zu.

7 Die Bedeutung von Cookies bei der Arbeit auf WiBeS

Beim Zugang über einen Internetbrowser werden Cookies gesetzt. Die Cookies bei Microsoft SharePoint dienen nur der Identifikation des Clients (Einzelplatzbenutzer), um die Kommunikation zwischen Client und SharePoint aufrechtzuerhalten. Ein Auslesen personenbezogener Daten ist nicht möglich.

8 Verantwortlichkeiten und Pflichten der NutzerInnen

Die Nutzer von WiBeS sind für den veröffentlichten Content (Texte, Bilder, Videos, Beiträge) selbst verantwortlich und tragen dafür Sorge, dass insbesondere keine Rechte Dritter (z.B. Urheber-, Persönlichkeitsrechte und Datenschutzbestimmungen) verletzt werden. Für die Inhalte und die Zulässigkeit von Beiträgen, die von WiBeS-Nutzern über WiBeS veröffentlicht, versendet, empfangen oder in einer sonstigen Form publiziert werden, übernimmt WiBeS keine Garantie und Haftung.

Eingeschlossen sind hierbei Links und E-Mail- Adressen, die von Mitgliedern innerhalb ihrer eigenen Beiträge veröffentlicht werden. Wir empfehlen daher innerhalb der schulischen Organisation eine „Sharing Policy“ zu erstellen und diese mit den schulischen Mitbestimmungsgremien abzustimmen.[9]

Über die Veröffentlichung des Namens und des Benutzernamens hinausgehende personenbezogene Daten bestimmt der Nutzer in seinem persönlichen Profil selbst. Für die unter seinem Benutzernamen erfolgten Handlungen ist der Nutzer verantwortlich (siehe Pkt. 9). Deshalb hat er das Passwort gemäß der Dataport-Passwort-Richtlinien für WiBeS geheim zu halten und regelmäßig zu ändern. Eine Weitergabe seiner Zugangsdaten an andere Personen ist nicht erlaubt.

Dies gilt ebenso für das Zugänglichmachen der Anmeldedaten für nicht zugangsberechtigte Dritte (z.B. durch die Weitergabe der persönlichen Zugangsdaten). Der Nutzer muss sich nach der Arbeit mit WiBeS sofort, das bedeutet unverzüglich, ausloggen, insbesondere bei Verwendung öffentlich zugänglicher PCs.

Weiterhin ist eine Registrierung mit einer alternativen E-Mail-Adresse für die Nutzung des Passwort-Service (PWS) erforderlich (siehe Pkt.4). WiBeS haftet nicht für Inhalte und für keinen Verlust oder Schaden, der durch die Benutzung von Inhalten entstanden ist. WiBeS überprüft und kontrolliert Inhalte grundsätzlich nicht, behält sich jedoch das Recht vor, Inhalte, die über die Domäne wibes.de zugänglich sind, zu entfernen, wenn sie gegen diese Nutzungsbedingungen verstoßen.

9 E-Mail-Verkehr

Jeder Nutzer von WiBeS erhält eine E-Mail-Adresse, welche ausschließlich für den dienstlichen bzw. schulischen Bereich vorgesehen ist.

10 Rechte an veröffentlichten Inhalten

Falls der Nutzer in einen öffentlich über die Einzelschule (Websitesammlung) zugänglichen Bereich einen Inhalt eingibt, ohne dass er die Rechte an diesem hat, gewährleistet er, dass der Eigentümer des Inhalts sich mit der Veröffentlichung einverstanden erklärt hat.

[9] https://dsgvo-gesetz.de/art-5-dsgvo/

11 Keine kommerzielle Nutzung der Serviceleistungen

Der Nutzer darf die angebotenen Dienste und konfigurierten Anwendungen von WiBeS oder Teile davon oder den Zugang zu den angebotenen Diensten und konfigurierten Anwendungen nicht kommerziell nutzen.

12 Beendigung

Die Nutzer können ihren Zugang zu jeder Zeit ohne Angabe von Gründen löschen lassen. Hierzu müssen sie eine Absprache mit dem WiBeS-Betreuer ihrer Schule treffen. Sie sind damit einverstanden, dass WiBeS ihnen gegenüber oder gegenüber Dritten nicht für die Beendigung des Zugangs zu den in Punkt 2 beschriebenen Leistungen haftbar gemacht werden kann.

Bei Beendigung der Nutzung von WiBeS werden spätestens nach einer Frist von 3 Monaten die E-Mail Adresse gestrichen und alle vorhandenen Nachrichten gelöscht. Dies betrifft auch die Daten der MySite. Ein Anspruch auf die Aufbewahrung vorhandener Daten bzw. Dateien besteht seitens des Nutzers nicht. WiBeS haftet nicht für etwaige Schäden, die durch die Löschung entstehen.

13 Geschäfte mit Dritten

Die Kommunikation oder Geschäftsbeziehungen mit kommerziellen Anbietern oder sonstigen Dritten, die der Nutzer im Rahmen der angebotenen Dienste und konfigurierten Anwendungen von WiBeS durchführen, finden ausschließlich im Verhältnis zwischen dem Nutzer und einem solchen Dritten statt. WiBeS ist für Verluste oder Schäden aus solchen Geschäften nicht verantwortlich und auch nicht haftbar.

14 Haftungsbeschränkung

WiBeS haftet nicht für das Verhalten von Nutzern oder sonstigen Dritten oder für Inhalte oder Erklärungen, die von Nutzern oder sonstigen Dritten im Rahmen der angebotenen Dienste und konfigurierten Anwendungen von WiBeS weitergegeben werden. WiBeS haftet auch nicht für Schäden, die aus der Nutzung oder Unmöglichkeit der Nutzung der angebotenen Dienste und konfigurierten Anwendungen entstehen.

15 Mitteilungen

Mitteilungen an den Nutzer werden entweder per E-Mail sowie über die Portalstartseite übermittelt. Mitteilungen an WiBeS können per E-Mail oder telefonisch übermittelt werden.

16 Salvatorische Klausel

Diese Nutzungsbedingungen sind online im Anmeldefenster von WiBeS und bei Nutzung des Passortservices zugänglich. Den Bestimmungen ist immer dann zuzustimmen, wenn sich Benutzer ein neues Passwort setzen. Die Nutzungsbedingungen kann jederzeit von WiBeS geändert werden, sofern dies sachlich begründet ist. Mit der Zustimmung zu diesen Nutzungsbedingungen erkennt der Nutzer die Gültigkeit jeder Einzelbestimmung für sich an, die Gültigkeit einer jeden Einzel-bestimmung wird nicht durch die Gültigkeit anderer Einzelbestimmungen beeinflusst. Änderungen treten mit der Online-Publizierung in Kraft.

Durch den fortgesetzten Gebrauch der WiBeS stimmen die Nutzer der geänderten Vereinbarung zu. Die Mitbestimmung der Personalräte bleibt davon unberührt.

18 Verstöße gegen diese Nutzungsbedingungen

Bei erwiesenen Verstößen gegen diese Nutzungsbedingungen werden geeignete Maßnahmen durch die Dienstvorgesetzten auf dem Dienstweg abgestimmt.

19 Wichtiger Hinweis zu allen Links

Mit Urteil vom 12. Mai 1998 - 312 O 85/98 – „Haftung für Links“ hat das Landgericht (LG) Hamburg entschieden, dass man durch die Anbringung eines Links, die Inhalte der gelinkten Seite ggf. mit zu verantworten hat. Dies kann - so das LG - nur dadurch verhindert werden, dass man sich ausdrücklich von diesen Inhalten distanziert. Hiermit distanzieren wir uns ausdrücklich von allen Inhalten aller gelinkten Seiten auf unserer Homepage und machen uns diese Inhalte nicht zu Eigen. Diese Erklärung gilt für alle auf dieser Website angebrachten Links. Für alle diese Links gilt: „WiBeS und alle hierfür Verantwortlichen betonen ausdrücklich, dass wir keinerlei Einfluss auf die Gestaltung und die Inhalte der gelinkten Seiten haben. Deshalb distanzieren wir uns hiermit ausdrücklich von allen Inhalten aller gelinkten Seiten innerhalb von WiBeS.de inklusive aller Unterseiten. Diese Erklärung gilt für alle auf WiBeS.de und in den WiBeS angebotenen Diensten und konfigurierten Anwendungen verwendeten Links und für alle Inhalte der Seiten, zu denen Links oder Banner von WiBeS.de und deren Nutzer führen.“

WiBeS-Team

Hamburger Institut für Berufliche Bildung (HIBB)

Wissensmanagement für Berufsbildende Schulen

Telefon: +49(40) 428 976 - 251
E-Fax: +49(40) 427 968 - 292
E-Mail: Ronald.Wiegand@wibes.de
(E-Mail: Ronald.Wiegand@hibb.hamburg.de)
www.HIBB.Hamburg.de

Hamburg, den 04.02..2019 / Version 5.0

20. Anhang: Clean Desk Policy (Anlage zu WiBeS-Nutzungsbedingungen)

a. T Sicherheit geht uns alle an!

In jeder Organisation werden mittlerweile Daten vorwiegend elektronisch verarbeitet. Die verarbeiteten Daten reichen von Schülerdaten, Lehrerdaten, Daten von Kooperationspartner, Bewerberdaten, und vor allem personenbezogene Daten (EU-DSGVO). Alle Datenkategorien sind besonders schützenswerte Daten. Diese Daten dürfen keinesfalls in die Hände von unbefugten Dritten fallen. Sei es aus Gründen des Datenschutzes, oder weil es sich um vertrauliche schulische Daten handelt. Datensicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar für den schulischen Erfolg. Schulische Daten müssen daher bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Vorkommisse.

Die nachfolgenden Punkte sind sowohl für die Schulen, in dem sie arbeiten von großer Bedeutung, aber auch sie persönlich profitieren privat von dieser Richtlinie. Mit ihrer Unterschrift bestätigen sie, dass sie diese Richtlinien beachten und umsetzen werden.

b. Sicherer Umgang mit personenbezogenen Daten

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschafts-zugehörigkeit. Sie sind besonders schützenswert. Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten ist nur unter Zustimmung des Betroffenen zulässig.

Bitte beachten sie folgende Punkte:

Personenbezogene Daten müssen geheim gehalten werden. Nur bei schriftlicher Zustimmung dürfen diese Daten an Dritte weitergegeben werden. Bei Weitergabe der Daten muss auf einen sicheren Kommunikationsweg geachtet werden. Ein unverschlüsseltes E-Mail erfüllt diese Anforderung NICHT. Nach dem Ausscheiden aus der Schule oder dem Wechsel der Arbeitsstelle dürfen sie personenbezogene Daten, die ihnen beruflich zugänglich gemacht wurden, nicht weitergegeben oder für andere Zwecke genutzt werden.

Unter der Clean Desk Policy versteht man, dass KuK und SuS und Mitarbeiterinnen und Mitarbeiter alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen, oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bitte beachten sie folgende Punkte:

- Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind (Schreibtisch, abschließbare Kästen, Datenträgersafe).
- Lassen sie keine Ausdrucke im Drucker/Kopierer liegen.
- Bewahren sie unter keinen Umständen Passwort-Notizen an Ihrem Arbeitsplatz auf.
- Sperren sie Ihren Computer, wenn sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten. In vielen Organisationen wird die Sitzung automatisch nach einer bestimmten Inaktivität getrennt.

c. Persönliche Passwörter

Stellen sie sich ein Passwort wie einen Schlüssel zu ihrer Wohnung oder zu ihrem Haus vor. Zuhause möchte sie auch ein gutes Schloss besitzen, welches vor einem unbefugten Zutritt schützt. Genauso verhalten sich auch Passwörter. Passwörter schützen vor unbefugten Zutritt.

Bitte beachten sie folgende Punkte:

- Verwenden sie nie das gleiche Passwort für unterschiedliche Zugänge.
- Verwenden sie z.B. eine Passwort-Datenbank (z.B. www.keepass.info).[10]
- Verwenden Sie die „Multifaktor Authentifizierung“ oder biometrische Authentifizierung da wo möglich.[11] [12]
- Verwenden sie Kennwörter, die mindestens 10 Zeichen und drei Kriterien haben. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen um halbwegs sicher zu sein.
- Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc. verwenden. Diese werden bei Angriffen zuerst ausprobiert.
- Verwenden sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geographische Begriffe etc. dürfen nicht verwendet werden.

[10] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

[11] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

[12] https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DiOS&hl=de

- Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passwort Eingabe erkannt werden.
- Geben sie ihr Passwort niemanden weiter! Auch Kollegen oder IT-Betreuung benötigen ihr Kennwort nicht.
- Ändern sie ihr Kennwort in regelmäßigen Abständen (mind. alle 90 Tage).
- Überlegen sie sich einen Satz und verwenden sie nur die Anfangsbuchstaben für ihr Passwort.
    - Die Arbeit beginnt jeden Tag um 7 Uhr - DAbjTu7U
    - Am Samstag arbeite ich von 9 bis 13 Uhr - ASaiv9-13U
- Sie sind für ihr Kennwort verantwortlich! Sollten sie den Verdacht haben, dass ein Dritter ihr Kennwort kennt, ändern sie dieses sofort. Sicherheitshinweise erhalten Sie unter www.bsi.de oder unter: https://www.bsi-fuer-buerger.de .

d. Verschlüsselte Kommunikation

- Bitte achten sie auf eine verschlüsselte Kommunikation. Ihr Browser beispielsweise signalisiert dies mit einem Schloss. Alle übermittelten Daten und alle Daten, die sie zum Beispiel in ein Formular auf dieser Webseite eingeben, sind demnach verschlüsselt. Die verschlüsselte Kommunikation mittels E-Mail gestaltet sich etwas schwieriger, da bei der Entwicklung der E-Mail keiner an die sichere/verschlüsselte Kommunikation gedacht hat. Bitte beachten sie, dass eine normale (unverschlüsselte) E-Mail KEINE sichere Kommunikation darstellt.
- Um diesen E-Mails dennoch etwas Sicherheit einzuhauchen, gibt es Erweiterungen, die vor dem Senden der E-Mail diese verschlüsselt und beim Empfänger automatisch entschlüsselt. Durch diese Technologie können auch sensible Daten per Mail versendet werden. Gängige Erweiterungen sind PGP oder S/MIME. Bitte setzen sie sich mit der IT Abteilung in Verbindung, um diese Technologie zu evaluieren. Viele E-Mail Provider bieten mittlerweile auch verschlüsselte E-Mail Accounts an. Fragen Sie Ihren Anbieter Support. Nutzen Sie daher, wenn möglich den sicheren WiBeS-E-Mail-Exchange Zugang.

e. Dokumente und Datenträger richtig entsorgen

Sorglos weggeworfene Dokumente stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente, Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD...) sicher entsorgt werden.

Für die sichere Entsorgung eignet sich ein Dokumenten-Schredder oder ein Dienstleistungsunternehmen, welches sich auf die sichere Entsorgung spezialisiert hat. Das Dienstleistungsunternehmen stellt ihnen anschließend ein Zertifikat aus, welches die fachgerechte Entsorgung bestätigt.[13]

Ihre Organisation muss im Rahmen der DSGVO Dokumentation (Technisch-Organisatorische Maßnahmen (TOM's), dies per Unterschrift bestätigen!

Bitte beachten sie folgende Punkte:

- Werfen sie Datenträger oder wichtige Dokumente auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger und Dokumente sicher entsorgt werden. Beachten sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.
- Übergeben sie die nicht mehr benötigten Datenträger den Verantwortlichen Ihrer IT-Abteilung bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist.

f. Speicherung von Daten

Bitte versichern sie sich, dass Daten nur an den dafür definierten Bereichen gespeichert werden. Die Daten sollten zumindest auf einem Netzlaufwerk, oder in einem dafür vorgesehenen Dokumentenmanagement gespeichert werden. Eine Speicherung auf lokalen Datenträgern wie die interne Festplatte in ihrem Rechner – gerne auch als Laufwerk C: bezeichnet -, oder angeschlossene USB Sticks dürfen dafür nicht verwendet werden.

g. Umgang mit mobilen IT-Geräten (BYOD)

Mobile IT Geräte (Notebooks, Smartphones…) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel.

Bitte beachten sie folgende Punkte:

- Lassen sie das Gerät nicht unbeaufsichtigt.
- Schützen Sie das mobile Endgerät durch biometrische Authentifizierung und /oder durch Kennwortschutz (Desktopsperre möglichst gering halten <1 Minute)
- Überlassen sie das Gerät nicht anderen Personen.

[13] https://dsgvo-gesetz.de/art-32-dsgvo/

- Achten sie bei Passwort-Eingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
- Verwenden sie ihren privaten Cloud-Speicher nicht für schulische Unternehmensdaten.
- Installieren sie nur Anwendungen, die ihnen als vertrauenswürdig und sicher bekannt sind und von ihrer IT-Abteilung frei gegeben wurden.
- Melden sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
- Achten sie auf eventuelle Daten- und Gesprächspaketvolumen um zusätzliche Kosten für das Unternehmen zu vermeiden.
- Speichern Sie niemals Passwörter unverschlüsselt auf einem mobilen Endgerät. Nutzen Sie dafür z.B. Passwort-Manager wie „Keepass“.[14]

h. Internetnutzung

Auch beim normalen Surfen im Internet lauern Gefahren, die nicht gleich als solche erkannt werden. Es liegt in ihrer eigenen Verantwortung, solche Bedrohungen zu erkennen und entsprechend darauf zu reagieren. Verfügen Sie über eine „Antiviren Suite“ Software, werden diese Gefahren frühzeitig erkannt. Dies auch bei Downloads aus dem Internet und Attachments in Outlook. Einfache kostenlose Programme unterstützen dies in der Regel nicht.

Bitte beachten sie folgende Punkte:

- Gebrauchen sie ihren Hausverstand! Wenn sie z.B. keinen Handy Vertrag mit A1 oder Telekom haben, handelt es sich bei eingegangen E-Mails von A1 oder Telekom meistens um betrügerische E-Mails.
- Übermitteln sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als Sicher (HTTPS) markiert wird.
- Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, sind grundsätzlich zu misstrauen.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist.
- Meiden sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird.

[14] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

- Rufen sie keine Websites mit pornographischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für ihr Unternehmen – nach sich ziehen. Fragen sie lieber einmal zu viel bei ihrer IT-Abteilung nach.

i. Protokollierung

- Zu beachten ist, dass jeder Datenverkehr einer Protokollierung und Auswertung unterliegt, um eventuelle Datenverletzungen oder Schadcodeverbreitung frühzeitig erkennen und unterbinden zu können. Die Auswertung erfolgt nur in Verbindung der Geschäftsleitung unter Wahrung des Datenschutzes.

j. SSL Interception

- Durch die Verwendung von verschlüsselten Verbindungen wird es leider auch Schadsoftware (Ransomware) ermöglicht, verschlüsselt und somit unentdeckt zu kommunizieren. Um dies zu verhindern, werden bestimmte Datenpakete an einem zentralen Punkt durchleuchtet. Davon ausgenommen sind Finanzdienstleister, Behörden, Rechtsanwälte, Gewerkschaften und Medizinische Einrichtungen.

k. E-Mail Nutzung

- E-Mail gehört zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle diese Form der Kommunikation zu nutzen. Somit landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten in ihrem Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des weltweiten E-Mail-Aufkommens aus.

Bitte beachten sie folgende Punkte:

- Öffnen sie keine E-Mails, wenn ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Öffnen sie niemals Dateianhänge, die ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?

- Öffnen sie keine E-Mails mit Spaßprogrammen, da diese Schadsoftware enthalten können.
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen sie auf keinen Fall weitergeben.
- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
- Beantworten sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen sie auch Ihre Kolleginnen und Kollegen über verdächtige Zusendungen. Besprechen sie die aktuellen E-Mails, die sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.
- Fragen sie ihre IT-Abteilungen, falls sie sich unsicher sind.
- Denken sie bei ihrem Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten, um die Absender über ihre Abwesenheit zu informieren.

I. Social Engineering

- Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt. Ein aktuelles Beispiel ist der Angriff auf die Firma FACC. Durch eine gefälschte E-Mail-Adresse wurden mehrere Millionen Euro erbeutet. Bis heute konnte der Angreifer nicht dingfest gemacht werden.
- Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu Ihrer IT-Abteilung zu gehören.

Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

Bitte beachten sie folgende Punkte:

- Seien sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag der Kollegin oder des Kollegen außergewöhnlich ist.
- Falls möglich, besprechen sie die Angelegenheit mit ihrem Kollegen oder mit ihrer Kollegin persönlich.
- Fragen sie bei verdächtigen E-Mail ihre IT-Abteilung.
- Bedenken sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
- Geben sie keine vertraulichen Informationen per Telefon oder E-Mail weiter.

m. Private Nutzung der IT

- Die Nutzung der IT für private Zwecke ist untersagt. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Smartphone etc.) als auch ihr Firmenpostfach (E-Mail) und den schulischen Internetanschluss. Sollte die private Nutzung von ihrer Seite notwendig sein, holen sie sich bitte eine schriftliche Ausnahmebestätigung von ihrem Vorgesetzten.

n. Warnungen und Fehlermeldungen

Warnungen oder Fehlermeldungen die sie selbst nicht verursacht haben, bzw. die sie nicht lösen können, müssen unverzüglich der IT Abteilung gemeldet werden.

o. Wechselmedien

Als Wechselmedien gelten alle externen Datenträger wie z.B. USB-Sticks, SD Karten, externe Festplatten, CD’s, DVD’s, Smartphones die per USB angeschlossen werden. Der Einsatz stellt ein großes Sicherheitsrisiko dar. Speziell wenn diese Datenträger aus externer Quelle standen.

Auf diesen Wechselmedien kann sich Schadsoftware verstecken, welche das gesamte Firmennetzwerk lahmlegen kann. Generell ist die Verwendung von Wechselmedien untersagt. Bitte beantragen sie eine Ausnahmengenehmigung, falls sie dennoch Wechselmedien verwenden müssen.

p. Installation von Applikationen

- Die Installation von Applikationen ist untersagt. Dies gilt sowohl für Windows Geräte (PC's, Notebooks, Server), aber auch für Firmeneigene Mobilgeräte wie Smartphone und Tablets. Falls sie eine Applikation benötigen, senden sie eine schriftliche Anfrage an ihre IT Abteilung. Auch harmlos wirkende Applikationen können Schadsoftware enthalten, oder sind lizenzrechtlich nicht für den schulischen Einsatz freigegeben.

q. Austritt aus der Schule

- Bei Austritt aus der Schule behält sich der Arbeitgeber das Recht vor, E-Mail-Adressen des ausscheidenden Mitarbeiters weiter zu verwenden, um den Unternehmensablauf nicht zu beeinträchtigen. Darüber hinaus verpflichtet sich der Mitarbeiter, sämtliche Dokumente, IT-Equipment und Unterlagen bei Austritt unaufgefordert der Schule bereit zu stellen. In einem Beschäftigungsverhältnis ist in der Regel der Arbeitgeber der Inhaber des generierten Geistigen Eigentums. Speziell im Hinblick auf Dokumente, Berechnungen oder dergleichen ist dies ein wesentlicher Punkt. Eine willkürliche Löschung von Dokumenten, E-Mails, oder sonstigen firmenrelevanten Daten ist untersagt.

.....

Ort, Datum

.....

Unterschrift MitarbeiterIn / SchülerIn