IT- Sicherheitskonzept für …… e.V.

1.
Einleitung

Der …… e.V. ist für IT-Sicherheit verantwortlich. Informations- und Kommunikationstechnik (IT) ist in heutiger Zeit ein unverzichtbares Instrument zur Erfüllung aller notwenigen Aufgaben im Rahmen der Vereinstätigkeit. IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Diese umfasst die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).
Die Vorgaben des Datenschutzes sind im Bundesdatenschutzgesetz in der jeweiligen aktuellen Form formuliert. Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung und den Umgang seiner personenbezogenen Daten in dem Recht beeinträchtigt wird,
selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").
Alle Beschäftigten sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten.
Alle Mitarbeitenden und sonstige relevante Personen (extern Beschäftigte und Projektmitarbeiter) werden systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult. Es sind technisch-organisatorische Verfahren zu nutzen, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in bestehende Bestandsverzeichnisse sicherzustellen. Mit dieser Richtlinie und der im Anhang enthaltenen Checkliste zur Informationssicherheit soll diesen Organisationen ein Werkzeug an die Hand gegeben werden. Dieses Dokument muss regelmäßig fortgeschrieben werden. Es bietet sich an, die Regelungen und die Checkliste quartalsweise oder in kürzeren Intervallen, mindestens aber einmal im Jahr zu überprüfen und ggf. anzupassen. Hierbei muss man sich der Tatsache bewusst sein, dass IT-Sicherheit kein statischer Zustand ist, sondern sich in einem stetigen Prozess fortentwickelt.
Zudem existieren in der Regel bereits unterschiedlich ausgeprägte IT-Standards (z. B. Datensicherung, Kennwortregelungen, Protokollierung). Es gibt z. T. Dienstleistungen, die durch Outsourcing betrieben werden. Informationssicherheit sorgt dafür, dass die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden. Vertraulichkeit schützen bedeutet, die IT-Systeme und Anwendungen so zu sichern, dass nur autorisierte Personen auf die verarbeiteten Daten Zugriff haben. Integrität schützt die Daten vor Manipulationen. Verfügbarkeit hingegen sorgt dafür, dass Daten im gewünschten Zeitraum zur Verfügung stehen und darauf zugegriffen werden kann.

2.
Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden.
Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen.
Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.
Ein Beispiel für eine Sensibilisierung der Mitarbeitenden „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz“ befindet sich im Anhang

3.
Datensicherungskonzept

Computersysteme und Datenträger (z. B. Festplatten, Speicherkarten) können ausfallen oder manipuliert werden. Durch Verlust oder Veränderungen von gespeicherten Daten können mitunter gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen werden Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen nicht verhindert, deren Auswirkungen können aber minimiert werden.

Die zu sichernden Daten und Anwendungen (hauptsächlich dezentral) müssen aufgelistet und jeweils einem Verantwortlichen zugordnet werden.

Backup-Datenträger müssen einerseits im Bedarfsfall schnell verfügbar sein, andererseits sollten sie räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Somit sind sie auch bei Notlagen, wie z. B. Brand oder Hochwasser verfügbar.

Hinweis:

Das zusätzliche Speichern auf einem vorzugsweise verschlüsselten USB-Stick könnte eine Datensicherung darstellen.

4.
Schutz vor Schadprogrammen

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden.
Es muss auf jedem IT-System (z. B. PC, Laptop) ein Viren -Schutzprogramm installiert werden. Automatische Updates müssen aktiviert sein. Dabei muss sichergestellt werden, dass auch die mobilen Endgeräte ausreichend geschützt sind. Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden. Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird (z. B. Webbrowser).

5.
Regelungen für Hard- und Software

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen ist es erforderlich, dass Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte Niveau der Informationssicherheit erreicht bzw. beibehalten wird.
Alle Mitarbeitenden müssen darüber informiert werden, dass nur explizit von der Einrichtung freigegebene und korrekt lizensierte Standardsoftware eingesetzt werden darf. Es darf nur solche Software eingesetzt werden, für das noch regelmäßige Sicherheitsupdate und -patches ausgeliefert werden.
Durch eine geeignete Benutzerkonten - und Rechteverwaltung wird sichergestellt, dass nur diejenigen Personen Zugriff auf IT-Systeme, Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.
Bei der normalen Nutzung der Clients darf nicht mit administrativen Rechten (Admin-Benutzer) gearbeitet werden. Dies ist nur zu administrativen Tätigkeiten zulässig, die unbedingt von normalen Aufgaben getrennt durchzuführen sind.
Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist es wichtig, dass sich die Mitarbeitenden vor der Nutzung per Passwort authentisieren müssen. Die Benutzer müssen über die dafür notwendigen Regelungen und deren Anwendung sowie deren Hintergründe explizit informiert
werden. Das Passwort bei IT-Systemen muss aus mindestens 8 Zeichen bestehen. Es muss sich aus Klein- und Großbuchstaben, sowie aus Zahlen oder Sonderzeichen zusammensetzen.
Bei der Beendigung von Arbeitsverhältnissen ist die geordnete Über- und Rückgabe der Geräte und Daten sicherzustellen.
Das sichere Löschen und Vernichten von Daten auf Datenträgern (z.B. Server, Clients, Netzkomponenten, Smartphones) muss vor der Aussonderung oder vor einer Weitergabe der Datenträger und Geräte vorgenommen werden.

6.
Büroraum / Lokaler Arbeitsplatz

Der Büroraum ist ein Raum, indem sich eine oder mehrere Personen aufhalten, um dort der Erledigung ihrer Aufgaben nachzugehen. Diese Aufgaben können (auch IT-unterstützt) aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.
Fenster und Türen sind zu verschließen, wenn ein Raum nicht besetzt ist. Büroräume müssen so ausgestattet sein, dass schutzbedürftige Datenträger und Dokumente weggeschlossen werden können. Dazu müssen beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke vorhanden sein.
Alle Mitarbeitenden müssen darauf hingewiesen werden, dass auch in Büroräumen die vorhandenen IT-Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden.
In Büros mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT -Systemen (z. B. Laptops) einzusetzen, da andernfalls die Gefahr besteht, dass solche Geräte in einem unbewachten Augenblick abhandenkommen.

7.
Mobiler Arbeitsplatz

Ein mobiler Arbeitsplatz kann auch z. B. von Telearbeitern, freien Mitarbeitern oder Selbstständigen sowie von Ehrenamtlichen genutzt werden. Bei einem mobilen Arbeitsplatz kann die infrastrukturelle Sicherheit nicht so vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist. Dienstliche Aufgaben werden häufig auch an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen durchgeführt. Die dabei verarbeitenden Informationen müssen angemessen geschützt werden (z. B. durch Sperren des Bildschirms oder Anbringen eines Sichtschutzes). Die Leistungsfähigkeit von mobilen IT-Systemen wie beispielsweise Laptops, Handys und PDAs wächst
ständig und lässt es zu, große Mengen geschäftsrelevanter Informationen außerhalb der Räume der jeweiligen Institution zu bearbeiten. Dabei ist zu beachten, dass meist die infrastrukturelle Sicherheit nicht der einer Büroumgebung entspricht. An mobilen Arbeitsplätzen sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert, z. B. mit einer Diebstahlsicherung versehen oder in Schränke geschlossen werden.
Beim Einsatz mobiler Geräte sind die Festplatten der Rechner grundsätzlich immer zu verschlüsseln.