IT-Richtline / IT-Sicherheitskonzept des NMWP.NRW e.V.

Der Vorstand des NMWP.NRW e.V. verabschiedet hiermit folgende Richtlinie zur Informationssicherheit:

Einleitung

(1) Als gemeinnütziger Verein verarbeiten wir eine Vielzahl von (insbesondere personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Vereinsmitgliedern, Behörden, Vertragspartnern, der Öffentlichkeit und sonstigen Dritten zu erfüllen. Dabei verarbeiten wir auch Daten, die einen hohen Schutzbedarf aufweisen und die vor der unberechtigten Kenntnisnahme durch Dritte besonders zu schützen sind. Die Sicherheit der Informationsverarbeitung spielt daher eine Schlüsselrolle für unsere Aufgabenerfüllung.

(2) Diese IT-Richtlinie soll die vom Verein getroffenen Maßnahmen zum Schutz von Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitglieder unterstützen und darüber hinaus eine grundlegende Information für alle Mitglieder und im Verein Mitwirkenden im Hinblick auf den Umgang mit Daten sein.

Geltungsbereich

(3) Diese Richtlinie gilt für den gesamten Verein, insbesondere aber für die Geschäftsstelle, die Arbeitsumgebung der Vorsitzenden und des Schatzmeisters und aller für den Verein stellvertretend agierenden Vorstandsmitglieder und sonstigen ehrenamtlich Tätigen.

(4) Auch externe Personen, die für unseren Verein tätig sind, sind verpflichtet, sich an diese Richtlinie zu halten.

(5) Der Verein wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat.

Einhaltung von Rechtsvorschriften

(6) Bei der Benutzung der IT-Systeme und Anwendungen, beim E-Mail-Verkehr und bei der redaktionellen wie technischen Administration der Webseite unseres Vereins sind von den in den Vereinsorganen tätigen Mitgliedern, allen voran vom Vorstand, die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit einzuhalten.

Sicherheitsorganisation

a. Personelle Maßnahmen

(7) Verantwortlich für die Sicherheitsorganisation ist der geschäftsführende Vorstand.

b. Organisatorische Maßnahmen

Arbeitsplatz

(8) Beim Verlassen des Arbeitsplatzes müssen die in den Vereinsorganen tätigen Mitglieder sich „abmelden“, so dass vor der erneuten Nutzung des IT-Systems oder der Anwendung eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

(9) 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.

IT-Geräte

(10) Auf den vom Verein bereitgestellten IT-Geräten ist nur die eigens dafür frei gegebene Software zu betreiben. Die Installation von zusätzlicher Software wie auch die Ablage von persönlichen Daten ist generell untersagt oder ist im Einzelfall durch den Vorstand zu genehmigen.

(11) Die in den Vereinsorganen tätigen Mitglieder, die zum Arbeit ihre private Hardware einsetzen, verpflichten sich, dass die vom Verein festgelegten „Regelungen zum Datenschutz“ nach allen Kräften eingehalten werden.

Schulung

(12) Der Vorstand trägt Sorge dafür, dass die an die an der Vorstandsarbeit beteiligten Personen die erforderlichen Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und Anwendungen (in erster Linie E-Mail-Zugriff und Pflege der Webseite) erforderlich sind.

c. Technische Maßnahmen

Passwort-Gebrauch

(13) Soweit technisch möglich sind alle IT-Systeme und Anwendungen erst nach hinreichender Authentifizierung des Nutzers zu nutzen. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort.

Schutz vor Schad-Inhalten

(14) Zum Schutz vor Schad-Inhalten ist auf allen IT-Geräten, auf denen Vereinsinformationen und insb. personenbezogene Daten der Mitglieder verarbeitet werden, ein Virenschutzprogramm einzusetzen.

(15) Die Postfächer der vom Verein eingerichteten zentralen E-Mail-Konten werden zentral geschützt. Insbesondere eingehende E-Mail-Kommunikation wird durch diese Vorrichtung überprüft. Dabei kann es im Einzelfall auch zur Löschung von E-Mails und Dateianhängen kommen.

Schutz vor unverlangter Werbung („Spam“)

(16) Zum Schutz vor unverlangter Werbung durch E-Mail werden die vom Verein eingerichteten zentralen E-Mail-Konten mit so genannten Spam-Filter versehen. Dadurch kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt oder gelöscht werden

Nutzung von E-Mail

(17) Die E-Mail-Adressen des NMWP.NRW e.V. dürfen nur für die den Verein betreffende Kommunikation genutzt werden.

Updates

(18) Automatische Updates in den Betriebssystemen und den Anwendungsprogrammen sowie automatische Updates der verwendeten Browser sind voreingestellt aktiviert. Die Einstellungen dürfen nur vom technischen Administrator verändert werden.

Backup von Daten

(19) Backups werden regelmäßig erstellt.

Internetpräsenz/Webseite

(20) Die Website des NMWP.NRW e.V wird bezüglich ihres Inhaltes und Aufbaus/Layouts durch den Vorstand bestimmt.

(21) Im Impressum der Website des NMWP.NRW e.V. wird der offiziell Verantwortliche benannt mit einem Verweis auf § 5 des Telemediengesetzes (TMG). Generell ist dies der Vorstandsvorsitzende, da dieser auch als verantwortlich im Vereinsregister eingetragen ist. Der Vorstand kann über eine Delegierung der Verantwortung entscheiden.

(22) Die Bearbeitung der Website ist über persönliche, mit Passwort geschützten Accounts möglich. Der Account wird spätestens gelöscht oder deaktiviert, wenn der Vorstand dem Beauftragten die Vollmacht zur Bearbeitung entzieht.

Verhalten bei Sicherheitsvorfällen

(23) Sollte ein in den Vereinsorganen tätiges Mitglied bemerken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieses sich unverzüglich an den Vorstandsvorsitzenden zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

Verbesserung der Sicherheit

(24) Diese IT-Richtinie wird regelmäßig auf ihre Aktualität und Wirksamkeit geprüft und angepasst.

Düsseldorf, den 15.06.2018