Standeskanzlei Graubünden
Chanzlia chantunala dal Grischun
Cancelleria dello Stato dei Grigioni

Richtlinie Informationssicherheit

E-Voting Graubünden

Klassifizierung	Keine
Autor	E-Voting Beauftragter
Version	1.1
Datum	17.05.2024

7001 Chur, Reichsgasse 35, Tel. 081 257 22 23, Tel. direkt , 081 257 21 41, www.staka.gr.ch

Änderungskontrolle

Version	Datum	Beschreibung	Name
1.0	29.09.2023	Freigegebene Version	E-Voting Beauftragter
1.1	17.05.2024	Anpassungen in Abschnitt 4.8 / formelle Anpassungen	E-Voting Beauftragter

Prüf-/Freigabestellen

Prüfer	Freigeber	Datum
Leitung Abteilung Services	Leitung Standeskanzlei	22.09.2023

Referenzierte Dokumente

Nr.	Dokument	Version
[1]	Kantonales Datenschutzgesetz (KDSG, BR 171.100) vom 10. Juni 2001	Stand vom 01.01.2019
[2]	Konzept E-Voting	Aktuelle Version
[3]	Richtlinie Risikomanagement	Aktuelle Version
[4]	Konzept Schulungen und interne Information	Aktuelle Version
[5]	Gesetz über das Arbeitsverhältnis der Mitarbeitenden des Kantons Graubünden (PG, BR 170.400) vom 14. Juni 2006	Stand vom 01.01.2023
[6]	eCH Standards und Architekturen für eGovernment Anwendungen Schweiz (eCH-0014 / SAGA.ch) https://www.ech.ch/de/standards/60144	Version 08.0 vom 13.09.2017
[7]	Hardware und Infrastruktur	Aktuelle Version
[8]	Verordnung der BK über die elektronische Stimmabgabe (VEleS, SR 161.116) vom 25. Mai 2022	Stand am 01.07.2022
[9]	Glossar	Aktuelle Version

Inhaltsverzeichnis

1 Einleitung

Ziel der vorliegenden Richtlinie ist es, das Management, die Grundsätze und die Massnahmen der Informationssicherheit für den Betrieb von E-Voting zu definieren. Dieses Dokument richtet sich an alle Verwaltungseinheiten des Kantons Graubünden, die an den Aktivitäten rund um E-Voting beteiligt sind, sowie an die betroffenen Drittparteien.

2 Ziele und Anforderungen

2.1 Ziele

Die allgemeinen Ziele des Managements der Informationssicherheit sind:

- Sicherung des elektronischen Stimmkanals für die Stimmberechtigten des Kantons Graubünden. Insbesondere müssen das Stimmgeheimnis und - mit der Verifizierbarkeit - die Korrektheit eines Urnengangs sichergestellt werden.
- Sicherstellung der Konformität der Umsetzung und des Betriebs der elektronischen Stimmabgabe mit dem kantonalen Recht und mit den, in den entsprechenden Verordnungen, definierten Anforderungen des Bundes.

2.2 Anforderungen an die Informationssicherheit

Das Management der Informationssicherheit muss mit den gesetzlichen und regulatorischen Anforderungen im Bereich der Informationssicherheit, des Datenschutzes und der Geschäftskontinuität in Zusammenhang mit der elektronischen Stimmabgabe konform sein:

- Datenschutzgesetz des Kantons Graubünden (siehe *referenziertes Dokument [1]*)
- Weisung IKT-Sicherheit in der kantonalen Verwaltung Graubünden
- Regulatorische Anforderungen des Bundes (siehe *referenziertes Dokument [2]; Abschnitt 2 – Rechtsgrundlagen*)

Das System für die elektronische Stimmabgabe gehört gemäss der Schutzbedarfsanalyse des Kantons, gestützt auf die Weisung "IKT-Sicherheit in der kantonalen Verwaltung Graubünden", der Kategorie "sehr hoher Schutzbedarf" an.

3 Management der Informationssicherheit

3.1 Organisation und Anwendungsbereich

Die Organisation des Managements der Informationssicherheit in Zusammenhang mit E-Voting ist deckungsgleich mit der Organisation des Betriebes von E-Voting, welche im Dokument "Konzept E-Voting" (siehe *referenziertes Dokument [2]*) definiert ist. Dieser Rahmen stellt gleichzeitig auch den Anwendungsbereich dar.

3.2 Rollen und Verantwortlichkeiten

Die Rollen und Zuständigkeiten sind im Dokument "Konzept E-Voting" (siehe *referenziertes Dokument [2])* definiert. Die beiden für das vorliegende Dokument relevanten Rollen sind die "Leitung der elektronischen Stimmabgabe" sowie die "Leitung der Standeskanzlei".

3.2.1 Verantwortlichkeiten

Die Verantwortlichkeiten für die Informationssicherheit sind grundsätzlich wie folgt definiert:

- Die Leitung der Standeskanzlei stellt sicher, dass die gesetzlichen Anforderungen für die Durchführung von E-Voting erfüllt sind und die Sicherheit der Informationen systematisch sowie nachweislich gewährleistet ist. Daraus ergeben sich insbesondere die folgenden Verantwortlichkeiten:
    - Sicherstellung, dass das Management der Informationssicherheit entsprechend der vorliegenden Richtlinie implementiert wird.
    - Pflege dieses Dokuments, damit es die Ziele der Standeskanzlei im Bereich der Informationssicherheit der elektronischen Stimmabgabe wiedergibt.
    - Sicherstellung, dass die Verantwortlichkeiten für die Informationssicherheit jederzeit zugewiesen sind und diese Zuständigkeiten innerhalb der Standeskanzlei bekanntgegeben werden.
    - Sicherstellung, Förderung und Erleichterung der Integration von "Good Practices" der Informationssicherheit in die Prozesse der elektronischen Stimmabgabe.
    - Sicherstellung der notwendigen personellen Ressourcen für das Funktionieren des Managements der Informationssicherheit sowie Unterstützung der entsprechenden Mitarbeitenden, damit diese zur Wirksamkeit des Managements der Informationssicherheit beitragen können.
    - Gewährleistung der Vertrauenswürdigkeit des in der elektronischen Stimmabgabe eingesetzten Personals.
    - Sicherstellung des Informationsflusses betreffend der Bedeutung eines effizienten Informationssicherheitsmanagements und der Erfüllung der Anforderungen.
    - Förderung einer kontinuierlichen Verbesserung.
- Die Leitung der elektronischen Stimmabgabe
    - ist für die operative Koordination des Managements der Informationssicherheit sowie für die Berichterstattung über die Anwendung der Richtlinie verantwortlich;
    - setzt die Schulungen und Sensibilisierungsprogramme zur Informationssicherheit für die Angestellten der Standeskanzlei und die betroffenen Dritten um;
    - pflegt Beziehungen zu den Behörden, die in einem Krisenfall eingreifen müssen.
    - Die Eigner der einzelnen Informationsressourcen verantworten die Massnahmen zum Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der jeweiligen Informationsressourcen (siehe *Abschnitt 4.2*).

3.3 Risikomanagement

Die Standeskanzlei muss die Risiken, welche die Informationssicherheit betreffen, erkennen, beurteilen, auswerten und allenfalls mitigieren.

Das Risikomanagement ist in der "Richtlinie Risikomanagement" (siehe *referenziertes Dokument [3])* definiert. Die Standeskanzlei pflegt eine umfangreiche Risikoplanung, -beurteilung und -behandlung auf der Basis der Methode OCTAVE Allegro[1].

[1] Siehe https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

3.4 Schulung, Sensibilisierung und Kommunikation

In Zusammenarbeit mit den betroffenen Personen innerhalb der Organisation muss die Leitung der Standeskanzlei sicherstellen, dass die Sensibilisierungsmassnahmen, die bei allen Personen der Standeskanzlei und bei Dritten, die im Rahmen der elektronischen Stimmabgabe aktiv sind, durchgeführt werden.

Die Sensibilisierungsmassnahmen werden so aufgesetzt, dass die beteiligten Personen ihren Beitrag zur Wirksamkeit des Managements der Informationssicherheit leisten können und die Kenntnisse der geltenden Regelungen, Richtlinien und Verfahren sowie die Folgen von Nichtkonformitäten zu den Anforderungen sichergestellt sind.

Die nötigen Massnahmen betreffend Schulung und Sensibilisierung werden im Dokument "Konzept Schulungen und interne Information" (siehe *referenziertes Dokument [4])* definiert. Die Nachweise für die Durchführung werden aufbewahrt.

3.5 Leistungsbeurteilung und Verbesserung

Stellt die Leitung der elektronischen Stimmabgabe fest, dass die Einhaltung der Richtlinie nicht erfüllt wird oder die implementierten Sicherheitsmassnahmen mangelhaft sind, muss er/sie:

- die festgestellten Abweichungen dokumentieren.
- sofortige Korrekturmassnahmen zur Begrenzung der Auswirkungen umsetzen.
- entscheiden, ob eine Analyse zur Ermittlung der Ursachen der Nichtkonformität oder Mängel durchgeführt werden muss.
- Massnahmen zur Behebung dieser Ursachen umsetzen.
- nachprüfen, ob die Korrekturmassnahmen wirksam sind.

Die Leitung der elektronischen Stimmabgabe muss die Dokumentation der Leistungsbeurteilung und Verbesserung gemäss den Organisationsvorschriften der Standeskanzlei aufbewahren.

4 Informationssicherheitsmassnahmen

Die folgenden Abschnitte definieren die spezifischen Vorgaben und Massnahmen für die relevanten Informationssicherheitsthemen.

4.1 Personal

Die kantonalen Mitarbeitenden sind an das Gesetz über das Arbeitsverhältnis der Mitarbeitenden des Kantons Graubünden (PG; BR 170.400; siehe *referenziertes Dokument [5]*) sowie die vorliegende Richtlinie gebunden. Im PG werden die Pflichten der kantonalen Mitarbeitenden geregelt (Abschnitt 4, Pflichten der Mitarbeitenden). Es wird festgehalten, dass sie die Interessen der Öffentlichkeit zu wahren sowie alles zu unterlassen haben, was diese beeinträchtigt oder beeinträchtigen könnte (Art. 48 Abs. 1). Die Mitarbeitenden unterstehen zudem einer Geheimhaltungspflicht (Art. 50). Für den Betrieb von E-Voting gibt es keine besonderen personalrechtlichen Vorgaben; es gelangen die genannten Rechtsgrundlagen zur Anwendung. Für allfällige externe Mitarbeitende wird die vorliegende Richtlinie per Vertrag verbindlich erklärt.

Die Leitung der Standeskanzlei führt eine Auflistung von Sicherheitsregeln für die elektronische Stimmabgabe. Alle an der elektronischen Stimmabgabe beteiligten Mitarbeitenden der Standeskanzlei sind verpflichtet, diese Regeln zu kennen und einzuhalten. Die wichtigsten Regeln

werden von der Leitung der Standeskanzlei allen Akteuren mindestens einmal pro Jahr zu Beginn eines Urnengangs (ca. 7 Wochen vor der Stimmabgabe) in Erinnerung gerufen.

Die Leitung der elektronischen Stimmabgabe definiert die Sicherheitsregeln, die für die Gemeinden relevant sind. Diese Sicherheitsregeln sind Bestandteil der Anleitung für die Gemeinden.

Die Leitung der elektronischen Stimmabgabe führt einen Schulungsplan für alle Personen der Standeskanzlei und für Dritte, die im Rahmen der elektronischen Stimmabgabe aktiv sind (siehe *Abschnitt 3.4*).

4.2 Asset Management

Die Leitung der elektronischen Stimmabgabe führt ein detailliertes Inventar der Informationsressourcen und der Container mit der Zuteilung der Eigner.

Die Informationsressourcen sind wie folgt klassifiziert:

- Stufe: nicht klassifiziert (die Daten benötigen keinen speziellen Schutz in puncto Vertraulichkeit)
- Stufe: vertraulich (schützenswerte Daten)
- Stufe: geheim (besonders schützenswerte Daten)

Die Leitung der elektronischen Stimmabgabe muss sicherstellen, dass die Abläufe (Initialisierung, Verwendung und Vernichtung) der Geräte und der Datenträger, die im Rahmen von E-Voting eingesetzt werden, konform mit den im Dokument "Hardware und Infrastruktur" (siehe *referenziertes Dokument [7])* definierten Prozessen sind.

Alle Daten, die für den Betrieb der elektronischen Stimmabgabe relevant sind, bleiben ausschliesslich in der Schweiz. Die Übermittlung der Daten zwischen der Post und dem Kanton oder zwischen dem Kanton und der Druckerei findet auf technischen Plattformen statt, die ausschliesslich in der Schweiz betrieben werden.

4.3 Kryptographie

Die Regeln zur Anwendung der kryptographischen Massnahmen für die elektronische Stimmabgabe (Prozess zur Generierung, Verwendung und Sicherung der kryptographischen Schlüssel) werden von der Post vorgegeben. Für die Wahl von Zufallswerten, namentlich für die Setup-Komponenten und Kontrollkomponenten, wird die Entropie durch die Software der Post sichergestellt. Der Kanton definiert das Seed für die öffentlichen Werte gemäss den Vorgaben der Post[2].

Die Übermittlung der druckfertigen Stimmrechtsausweise an die Druckerei erfolgt verschlüsselt und signiert. Der Kanton setzt kryptographische Algorithmen ein, die konform zum Standard eCH-0014 sind (siehe *referenziertes Dokument [6]*).

Alle vom Kanton verwendeten elektronischen Zertifikate werden nach besten Praktiken verwaltet.

Das Zertifikat zum Signieren der Stimmrechtsausweise wird vom Kanton erstellt.

Für den Austausch von Zertifikaten gilt generell, dass die Authentizität der Zertifikate mittels Fingerprint geprüft werden muss. Dazu müssen das Zertifikat und der Fingerprint auf separatem Weg übermittelt werden. Bei Zertifikaten von vertrauenswürdigen Komponenten nach Ziffer 2 der Verordnung der BK über die elektronische Stimmabgabe (VEleS) ist gemäss Ziffer 3.8 der VEleS

[2] Cryptographic Primitives of the Swiss Post Voting System, Pseudo-code Specification, V1.4.0, Abschnitt 8.2 (https://gitlab.com/swisspost-evoting/crypto-primitives/crypto-primitives/-/blob/master/Crypto-Primitives-Specification.pdf)

ein manueller Prozess vorzusehen. Dies wird sichergestellt, indem der Fingerprint physisch übergeben wird. Ist eine physische Übergabe nicht möglich, wird der Fingerprint über einen sicheren elektronischen Kanal (z.B. Threema) geliefert und in einem Online-Meeting verifiziert. Die privaten Schlüssel der Zertifikate werden nur auf Offline-Computern oder verschlüsselten Datenträgern des Kantons gespeichert. Beim Zugriff und der Verwendung ist das 4-Augen-Prinzip sichergestellt.

Alle Passwörter, die für den Betrieb von E-Voting notwendig sind, müssen nach dem Zufallsprinzip und mit einer genügenden Länge generiert werden. Die Länge der Passwörter für die Computer muss mind. 13 Zeichen betragen. Für die Passwörter des Urnengangs wird ein Passwort mit 50 Zeichen[3] generiert und dabei ausreichend Entropie sichergestellt (mittels Mausbewegung und Tastatureingabe).

4.4 Physische Sicherheit

Die Zutrittskontrolle und Schutzmassnahmen der Räumlichkeiten werden im Dokument "Hardware und Infrastruktur" (siehe *referenziertes Dokument [7])* definiert.

Die physische Sicherung und die spezifische Aufbewahrung der Geräte und Datenträger, die bei der elektronischen Stimmabgabe verwendet werden, wird im Dokument "Hardware und Infrastruktur" (siehe *referenziertes Dokument [7])* beschrieben. Grundsätzlich werden während und ausserhalb eines Urnengangs alle physischen Elemente im Safe der Standeskanzlei aufbewahrt. Es ist sichergestellt, dass der Safe nicht durch nur eine Person geöffnet werden kann (4-Augen-Prinzip). Das Electoral-Board erhält das vollständige Protokoll der Aufbewahrung der Geräte und überprüft es. Das Electoral-Board kann die Einhaltung der Massnahmen überprüfen.

Die Wartung der Computer wird ebenfalls im Dokument "Hardware und Infrastruktur" (siehe *referenziertes Dokument [7])* beschrieben.

4.5 Betriebssicherheit

Alle in dieser Richtlinie aufgeführten Verfahren sind in der für den Kanton Graubünden geltenden Dokumentvorlage zu dokumentieren. Die entsprechende Dokumentation entspricht den Anforderungen und Vorgaben des Dokumentenmanagements. Die dokumentierten Verfahren sind den zuständigen Personen zur Verfügung zu stellen.

Für sämtliche involvierte Rollen wird immer eine Stellvertretung definiert. Die Präsenz der entsprechenden Personen für die relevante Periode wird vor dem Urnengang in einer Personalliste definiert.

Während des Urnengangs wird regelmässig ein Backup der Offline-Geräte durchgeführt, damit der Urnengang trotz allfälliger Ausfälle durchgeführt werden kann (siehe *referenziertes Dokument [7]*). Die Backup-Prozedur wird bei jedem Release, aber mind. einmal pro Jahr getestet.

Nach jedem Urnengang sind sämtliche Informationen auf den im Rahmen der elektronischen Stimmabgabe eingesetzten Geräten mit sicheren Löschmitteln zu vernichten. Dieser Prozessschritt wird im Dokument "Hardware und Infrastruktur" (siehe *referenziertes Dokument [7])* beschrieben.

[3] Die Bit-Länge der Passwörter muss dem Sicherheitslevel entsprechen. Im E-Voting-System gilt ein Sicherheitslevel von 128 bits. Bei 7-bit pro Zeichen wäre somit bereits ein Passwort mit einer Länge von 19 Zeichen genügend.

4.6 Aufgabentrennung

Betreffend Aufgabentrennung gemäss Anhang der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe unterliegen alle Vorgänge in Hochrisikobereichen sowie alle manuellen Operationen im Zusammenhang mit der elektronischen Urne dem 4-Augen-Prinzip.

4.7 Zugriffskontrolle

Der Zugriff auf und die Verwendung von vertrauenswürdigen Komponenten oder von Datenträgern mit kritischen Daten wird protokolliert und erfolgt im 4-Augen-Prinzip (siehe *Abschnitt 4.4* und *Abschnitt 4.6*). Manuelle Operationen im Zusammenhang mit der elektronischen Urne (z.B. Start der Auszählung) werden explizit authentifiziert.

4.8 Umgang mit Informationssicherheitsvorfällen

Die Leitung der elektronischen Stimmabgabe listet alle Informationssicherheitsvorfälle, die während oder ausserhalb der Stimmperiode auftreten, auf und dokumentiert diese. Die Liste wird ebenfalls dem Electoral-Board zur Verfügung gestellt.

Die Post, als Systemanbieterin, überwacht die Lage im Bereich der Informationssicherheit und arbeitet eng mit dem Bundesamt für Cybersicherheit (BACS) zusammen. Sie gibt die relevanten Meldungen und Empfehlungen an die Leitung der elektronischen Stimmabgabe weiter. Auch die kantonale Informatik überwacht die Lage im Bereich der Informationssicherheit und informiert die Leitung der elektronischen Stimmabgabe.

4.9 Lieferantenmanagement

Der Kanton hat mit allen Lieferanten, die im Betrieb der elektronischen Stimmabgaben involviert sind (insb. die Schweizerische Post und die Druckerei), schriftliche Verträge abgeschlossen.

Die Verträge stellen sicher, dass die Lieferanten die Rechtsgrundlagen berücksichtigen und die Vorgaben bezüglich Informationssicherheit einhalten. Die Lieferanten integrieren die Risiken aus der kantonalen Risikobeurteilung, von denen sie betroffen sind, in ihr Risiko-Portfolio und sind für die Umsetzung allfälliger Massnahmen zuständig. Der Kanton hat jederzeit die Möglichkeit, Informationen über die Umsetzung der Anforderungen zu erhalten oder die Umsetzung vor Ort zu kontrollieren.

Die Verträge werden regelmässig überprüft (u.a. Berücksichtigung von neuen Erkenntnissen aus der Überprüfung der Risikobeurteilung).

4.10 Change Management

Anpassungen an der Infrastruktur des Kantons, an Zugangs- und Zugriffsrechten sowie an der Infrastruktur der Post dürfen nur ausserhalb von Urnengängen stattfinden. Während eines Urnengangs sind keine Änderungen erlaubt.

Im Falle eines Notfalls (z.B. eine Schwachstelle wird bekannt) kann eine Ausnahme durch die Leitung der elektronischen Stimmabgabe bewilligt werden. Bei der Ausnahme muss berücksichtigt werden, dass die dadurch erwarteten Vorteile gegenüber den möglichen Gefahren überwiegen. Die Ausnahme wird dokumentiert und das Electoral-Board informiert (siehe auch *Abschnitt 4.8*).

4.11 Kommunikationssicherheit

Die Netzwerk-Komponenten werden von der IT des Kantons gemäss den kantonalen Standards betrieben und gesichert. Der Online-Computer darf im Netzwerk des Kantons nicht sichtbar sein, und darf nur die von der Leitung der elektronischen Stimmabgabe vorgegebenen dezidierten IP-Adressen erreichen. Die Offline-Computer dürfen nie mit dem Netzwerk/Internet verbunden sein.

5 Kommunikation der Regelung

Die Leitung der Standeskanzlei ist dafür verantwortlich, dass die Angestellten der Standeskanzlei und die Drittparteien, die von der elektronischen Stimmabgabe betroffen sind, mit den in dieser Richtlinie aufgeführten Regelungen vertraut sind.

6 Gültigkeit und Dokumentenmanagement

Dieses Dokument ist gültig ab dem 1. Dezember 2023.

Inhaberin dieses Dokuments ist die Leitung der Standeskanzlei, die das Dokument mindestens alle 3 Jahren überprüft und, wenn nötig, aktualisiert.