

CHECKLIST · TOMORIS TOOLBOX

Information Security in the Municipality: Checklist for Basic Protection

Responsibility, overview, accounts, updates, data backup, service providers and reporting points, based on the BSI municipal profile and the Austrian Information Security Handbook

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/gemeinde-informationssicherheit-checkliste

AT A GLANCE

§ 24

NISG 2026, para. 3: municipalities outside administration

Art. 32

GDPR: security of processing applies

Art. 37

GDPR: data protection officers for public authorities

GovCERT

Reporting point for public administration

WHO IT IS FOR

- Mayors who bear the responsibility
- Municipal office directors who organize procedures and responsibilities in the municipal office
- Municipal IT and IT service providers for municipalities
- Municipal associations and small public institutions

WHAT THIS COVERS

Municipal offices process citizens' personal data every day, often with little in-house IT staff and many external service providers. This checklist brings together basic protection for municipalities: who is responsible, what overview is needed, how accounts, updates, malware protection and data backup should be managed, what to look out for with remote maintenance, cloud and outsourcing, and whom to contact in an incident. It is based on the Austrian Information Security Handbook, the BSI profile Basis-Absicherung Kommunalverwaltung (basic protection for municipal administration) and the GDPR, and explains the role the NISG 2026 plays for municipalities.

This checklist is a TOMORIS recommendation and does not replace legal advice. The BSI profile comes from Germany and serves as a model. The GDPR, the NISG 2026 and the state and federal law applicable to your municipality in their current versions are decisive; whether municipally owned entities fall under the NISG 2026 must be reviewed case by case.

CONTENTS

01	Starting point for municipalities	2
02	Responsibility and organization	3
03	Overview of systems, procedures and partners	4
04	Accounts, updates, malware, data backup	4
05	Remote maintenance, cloud and external service providers	5
06	Security incidents and reporting points	5
07	Involving employees	6
08	Roadmap in five steps	7
09	Sources	8

01

Starting point for municipalities

What applies legally and which guides help

NISG 2026

Municipalities and municipal associations are expressly excluded from the public administration sector (§ 24 para. 3 NISG 2026 (Austrian Network and Information Systems Security Act 2026)). The NIS 2 Directive would have allowed Member States to include the local level (Art. 2(5)(a)). Whether municipal entities are covered in another sector must be reviewed separately.

GDPR	Applies to every municipality: appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32), and the obligation for public authorities and bodies to designate a data protection officer (Art. 37(1)(a)).
Austrian Information Security Handbook	Published by the Federal Chancellery and A-SIT, version 4.4.0 of November 6, 2023; describes how to build an information security management system in companies and public administration.
BSI profile Basis-Absicherung Kommunalverwaltung	German profile, version 4.0 of November 13, 2023, developed by the municipal basic protection working group with the municipal umbrella associations and published by the BSI; defines minimum measures for municipal administrations as a starting point. For Austria, a readily transferable model, not a legal obligation.

The checklist is a TOMORIS recommendation and follows the guides mentioned. The BSI profile expressly sees itself as a starting point: in the medium term, a security concept based on standard protection should build on it, because municipalities regularly process data with higher protection needs.

02 —

Responsibility and organization

Who is responsible, even when one person has several roles

- ☐ The mayor or the municipal office director takes responsibility for information security and provides resources (BSI profile, target group; Handbook, management responsibility).
- ☐ A responsible person named who drives the topic forward (BSI profile on ISMS.1.A4).
- ☐ Information security policy adopted and communicated; for this, the BSI profile refers to a separate guide for municipal administrations (BSI profile, framework conditions).
- ☐ Responsibilities defined; the same person may take on several tasks if the necessary responsibilities are defined (BSI profile on ORP.1).
- ☐ Contact person for difficult technical security questions designated; this can be an external service provider (BSI profile on ORP.1.A15).
- ☐ Data protection officer designated and involved in security questions at an early stage (Art. 37 GDPR; BSI profile on CON.2).
- ☐ Overview of the legal and contractual requirements for the municipal office (BSI profile, ORP.5).

03 —

Overview of systems, procedures and partners

What you need to know before you can protect it

- ☐ List of all sites and systems: municipal office, building yard, school, kindergarten, servers, workstations, network devices, printers.
- ☐ List of specialized applications and online services with responsible persons and providers.
- ☐ List of external service providers and cloud services with access rights and contracts.
- ☐ Protection needs assessed; for personal data in municipalities, they are usually higher than basic protection (BSI profile, protection needs).
- ☐ Procedures with special legal requirements marked; they need additional measures (BSI profile, recommended action).

The lists are the basis for all further points: for updates, data backup, permissions and emergencies. Keep them up to date and available even if the IT fails.

04 —

Accounts, updates, malware, data backup

Technical basic protection according to the BSI modules

Technical basic protection (requirements according to the BSI profile Basis-Absicherung Kommunalverwaltung)

AREA	WHAT SHOULD BE IN PLACE	MODULE
Accounts and rights	Set up and delete users in a controlled manner, grant, change, revoke and document permissions, separate functions, regulate password use and login; everyone instructed in the login procedures	ORP.4.A1 to A9, A22, A23, A19
Administration	Controlled administration, separate roles for application and system administration; external administrators also implement the module	OPS.1.1.2
Updates	Concept for patches and changes, responsibilities, handling of automatic updates, regular updating	OPS.1.1.3.A1 to A3, A15
Malware	Antivirus protection that users cannot disable; employees know the contact person in case of suspicion	OPS.1.1.4
Data backup	Identify influencing factors, define procedures and plans, back up regularly, protect and securely store backups, test regularly; take local hazards such as flooding into account for the storage location	CON.3.A1, A2, A4, A5, A12, A14, A15

Encryption and deletion

Cryptographic concept for personal data and communication; controlled deletion and destruction

CON.1, CON.6

Check your data backup with a copy that is separated from attacks and disruptions in the municipal office, and test the restore. The TOMORIS backup checklist 3-2-1-1-0 contains details on the procedure.

05

Remote maintenance, cloud and external service providers

Responsibility remains with the municipal office

- ☐ Remote maintenance only with current protocols classified as secure and defined tools; procedures regulated (BSI profile on OPS.1.2.5.A8, A9).
- ☐ Remote maintenance by third parties recorded and contractually regulated; documentation of access protected from unauthorized persons (OPS.1.2.5.A7, A19).
- ☐ Before procuring cloud services, requirements defined, data protection officer involved early, contract covering service, responsible persons, nature and location of processing (OPS.2.2.A2, A8, A9).
- ☐ Requirements for cloud services checked regularly against current evidence; termination already regulated at the start of the contract (OPS.2.2.A13, A14).
- ☐ With outsourcing, responsibility for information security remains with the authority; requirements defined in advance, exit strategy in the contract (BSI profile on OPS.2.3).
- ☐ For sensitive data, confidentiality agreed with service providers (BSI profile on OPS.2.3.A4); where a service provider processes personal data on your behalf, a data processing agreement (DPA) under Art. 28 GDPR.

06

Security incidents and reporting points

Whom to notify and how you are prepared

The BSI profile provides for the basic requirements of incident handling: define what a security incident is, set a policy and responsibilities, inform those affected, resolve incidents and restore the operating environment securely (DER.2.1.A1 to A6). For complete basic protection, business continuity management is added (DER.4).

Contact points in Austria (according to their own information)

ORGANIZATION	PURPOSE	CONTACT
GovCERT Austria	Computer emergency response team for public administration; reporting of other incidents in public administration, voluntary for municipalities	reports@govcert.gv.at
CERT.at	National CERT, contact for IT security, coordinates in case of attacks	team@cert.at, reports@cert.at
Federal Criminal Police Office	Tips and help in case of suspected cybercrime; file criminal complaints not by email but at any police station	against-cybercrime@bmi.gv.at
Austrian Data Protection Authority (Datenschutzbehörde)	Notification of a personal data breach, where feasible within 72 hours (Art. 33 GDPR)	Online or PDF form of the Data Protection Authority

Emergency contacts for your municipality (to fill in)

ROLE	NAME	REACHABLE AT
Mayor	_____	_____
Municipal office director	_____	_____
IT owner	_____	_____
IT service provider, emergency number	_____	_____
Data protection officer	_____	_____

Public administration organizations can take part in the active information exchange with GovCERT Austria; the Federal Ministry of the Interior decides on participation, and the organization names two contact persons.

07

Involving employees

Awareness, onboarding, offboarding and working from home

- ☐ Management sensitized, employees instructed in the secure use of IT and trained according to their tasks; on an ongoing basis, not just once (BSI profile on ORP.3.A1, A3, A6).
- ☐ Onboarding and offboarding regulated: accounts, rights and keys are granted and revoked in good time (BSI profile, ORP.2 and ORP.4).
- ☐ Working from home only according to rules, if used (BSI profile, OPS.1.2.4).

- ☐ Everyone knows whom to report a suspected malware infection or an incident to (BSI profile on OPS.1.1.4.A7).

08 —

Roadmap in five steps

From getting started to ongoing security management, TOMORIS recommendation

- 1 **Clarify responsibility**
Management decides, a responsible person is named, data protection officers are involved.
- 2 **Create an overview**
Record systems, specialized applications, service providers and contracts.
- 3 **Implement basic protection**
Work through the points in this checklist, starting with data backup, updates, accounts and remote maintenance.
- 4 **Prepare for emergencies**
Record contacts, procedures and recovery, for example with the IT emergency manual template, and practice once a year.
- 5 **Develop further**
In the medium term, build a security concept based on standard protection or a management system based on the Austrian Information Security Handbook.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

09 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
§ 8 para. 4, § 24 para. 3, § 46, accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1000942025
- 2 **Directive (EU) 2022/2555 (NIS 2 Directive), German version on EUR-Lex**
Art. 2(5)(a), accessed October 25, 2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 3 **Regulation (EU) 2016/679 (GDPR), German version on EUR-Lex**
Art. 28, 32, 33 and 37, accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 4 **Austrian Data Protection Authority: data breach notification**
Reporting channels and form, accessed October 25, 2026
dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach
- 5 **Austrian Information Security Handbook, version 4.4.0 (November 6, 2023), Federal Chancellery and A-SIT**
Introduction and management summary, accessed October 25, 2026
www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf
- 6 **BSI: IT-Grundschutz profile Basis-Absicherung Kommunalverwaltung, version 4.0 (November 13, 2023)**
Sections 5, 6 and 9.1, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/IT-Grundschutz-Profil-Basis-Absicherung-Kommunalverwaltung.pdf
- 7 **BSI IT-Grundschutz-Kompendium, module DER.2.1 Handling Security Incidents (Edition 2023)**
Basic requirements A1 to A6, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium.pdf
- 8 **GovCERT Austria: home page, reporting of other incidents, participation and services**
Mission, reporting address, participation in information exchange, accessed October 25, 2026
www.govcert.gv.at
- 9 **CERT.at: About us**
Role as national CERT, contact, accessed October 25, 2026
www.cert.at/de/ueber-uns
- 10 **Federal Criminal Police Office: Cybercrime Competence Center and reporting point against cybercrime**
Reporting point for cybercrime, accessed October 25, 2026
www.bundeskriminalamt.at/306/start.html