GRC+

Information Security Statement

CLASSIFICATION	VERSION	IN EFFECT FROM
PUBLIC	2.1	21 August 2026

LATEST VERSION
grc.plus/trust

Check this address before you rely on a printed or saved copy.

© 2026 GRC+

Document Control

FIELD	VALUE
Classification	PUBLIC: may be shared with anyone
Version	2.1
In effect from	21 August 2026
Latest version	grc.plus/trust

© 2026 GRC+

Contents

1	Governance	4
2	Access	5
3	Working with us	5
4	Client data	5
5	Devices and systems	6
6	Email and meetings	6
7	Monitoring	7
8	Incidents	7
9	Suppliers	7
10	Reporting a vulnerability	8

© 2026 GRC+

We advise clients on information securityProtecting information and the systems that handle it so that only authorised people can access it, it remains accurate and complete, and it is available when needed. These aims are called confidentiality, integrity and availability. Information security combines organisational requirements, staff practices and technical safeguards to reduce risks such as disclosure, alteration, disruption or destruction., so our own security has to hold up to the same questions. This statement summarises how GRC PLUS B.V. protects the information clients trust us with. Clients can request more detail, including completed security questionnaires, under a confidentialityThe information-security property of keeping information from being disclosed to people, organisations or systems that are not authorised to receive it. Access restrictions and encryption help preserve confidentiality when information is stored, sent or processed. It concerns who can see information; it does not by itself ensure that the information is accurate or that a service remains available. agreement.

1 Governance

- Our information securityProtecting information and the systems that handle it so that only authorised people can access it, it remains accurate and complete, and it is available when needed. These aims are called confidentiality, integrity and availability. Information security combines organisational requirements, staff practices and technical safeguards to reduce risks such as disclosure, alteration, disruption or destruction. management is based on ISO/IEC 27001Information Security, Cybersecurity and Privacy Protection: Information Security Management Systems: Requirements, with controls selected from ISO/IEC 27002Information Security, Cybersecurity and Privacy Protection: Information Security Controls.
- Management is accountable for information securityProtecting information and the systems that handle it so that only authorised people can access it, it remains accurate and complete, and it is available when needed. These aims are called confidentiality, integrity and availability. Information security combines organisational requirements, staff practices and technical safeguards to reduce risks such as disclosure, alteration, disruption or destruction.. Risks are reviewed at least every year and when something important changes.
- Our security configuration is kept as a documented baseline. Changes are assessed for their impact before they are made, and the decision is recorded.
- Everyone who works for us signs a confidentialityThe information-security property of keeping information from being disclosed to people, organisations or systems that are not authorised to receive it. Access restrictions and encryption help preserve confidentiality when information is stored, sent or processed. It concerns who can see information; it does not by itself ensure that the information is accurate or that a service remains available. agreement and follows our security requirements from the first day.

© 2026 GRC+

2 Access

- Strong multi-factor authenticationAuthentication through verification of at least two different types of factor: something a person knows, such as a password; something they have, such as a token; or something they are, such as a biometric. NIS2, PCI DSS, the NYDFS regulation and the FTC Safeguards Rule call for it. on every account, with phishingAn attack that impersonates a trusted person or organisation through electronic communications, often an email or a fake website, to trick someone into revealing information such as passwords or bank details. The attacker uses apparent familiarity or credibility to persuade the person to respond. Training simulations practise recognising these deceptive requests.-resistant methods for privileged access.
- Outdated sign-in methods are blocked, and unusual sign-ins are challenged or refused.
- Access only to the systems and client data a person needs, reviewed regularly and removed on the day someone leaves.
- Administrative rights are limited to named people, and their use is logged and monitored. No shared accounts.
- Our cloud provider’s engineers cannot access our data without our explicit approval.

3 Working with us

- Client contacts who collaborate in our workspace confirm their identity with multi-factor authenticationAuthentication through verification of at least two different types of factor: something a person knows, such as a password; something they have, such as a token; or something they are, such as a biometric. NIS2, PCI DSS, the NYDFS regulation and the FTC Safeguards Rule call for it. registered with us, and accept our collaboration notice before first access.
- Documents are shared with named people only. Anonymous links are not used.
- External access is time-limited and reviewed regularly. Access that is no longer used is removed.

4 Client data

- Client data is stored in approved systems only, never on personal devices or personal accounts.
- Information is classified by sensitivity. The most sensitive material is encrypted so that only the people it was shared with can open it.
- Controls detect and stop client personal and financial data leaving through unapproved

© 2026 GRC+

channels.

- Stored data is protected against unauthorised deletion and retained in line with our legal obligations.
- Where we process personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. for a client, a data processing agreementA contract setting out how a processor handles personal data on a controller's behalf. Under GDPR Article 28(3), the processing must be governed by a contract or another binding legal act with specified terms. sets out what we do and which sub-processors we use.
- When an engagement ends, we return or delete client data as agreed, keeping only what the law or professional standards require.
- Client confidential data goes into AIArtificial Intelligence tools only under the conditions in our responsible AI statement.

5 Devices and systems

- Company devices are centrally managed, encrypted, kept up to date and protected by endpoint detection and responseSecurity solutions deployed on endpoints, such as laptops and servers, to detect and respond to malicious activity. CISA advises using EDR or application allowlisting on all assets and considering EDR for cloud resources..
- On mobile devices, work data stays inside protected apps and can be removed without touching personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity..
- Cloud services are chosen for their security and for keeping data in the EU where possible, and configured to a documented baseline.
- Our website runs on managed hosting with web application firewall protection, daily backupsBackup and security monitoring.

6 Email and meetings

- Our domains use industry-standard email authentication, which makes it hard to send email that pretends to come from us.
- Incoming email is screened for phishingAn attack that impersonates a trusted person or organisation through electronic communications, often an email or a fake website, to trick

© 2026 GRC+

someone into revealing information such as passwords or bank details. The attacker uses apparent familiarity or credibility to persuade the person to respond. Training simulations practise recognising these deceptive requests. and malwareMalicious Software before it reaches anyone.

- Confidential correspondence can be sent encrypted, and access to it can be withdrawn.
- External participants are admitted to meetings by the organiser. Sensitive meetings get additional protection.

7 Monitoring

Security-relevant activity across our systems is logged and monitored, and alerts are investigated promptly. Logs are kept long enough to support an investigation.

8 Incidents

We keep an incident response planA written set of instructions for detecting and handling cybersecurity incidents and limiting their consequences. It gives the organisation a prepared approach to follow when systems or information are attacked. In practice, it should make clear who acts, how decisions and communications are handled, and how the response is coordinated. The plan supports the people doing the response work.. If an incident affects a client's information, we tell the client without undue delay, and for a personal data breachA breach of security leading to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data. A controller must notify the supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless it is unlikely to result in a risk to people's rights and freedoms. within 24 hours of becoming aware of it, so the client can meet its own reporting duties. Report a suspected incident to security@grc.plus.

9 Suppliers

Suppliers who handle our or our clients' information are assessed before we use them and bound by our supplier code of conduct.

© 2026 GRC+

10 Reporting a vulnerability

See our responsible disclosure policy.

Is this the latest version?
Scan the code or open grc.plus/trust. Version 2.1 was in effect from 21 August 2026.

This PDF is saved as PDF/A-1b for archiving. © 2026 GRC+

END OF DOCUMENT