Prepare a security report that can be investigated.

Describe the affected behaviour and a safe reproduction without sharing credentials or unnecessary customer information.

Security report contents

Include	Safe level of detail
Affected location	The public route, component or version involved
Observed behaviour	What happened and why it may be a security issue
Reproduction	Minimal steps using your own authorised test data
Impact	The access or action the behaviour could permit

Minimise sensitive material

Redact tokens, passwords and unrelated personal information. Do not copy customer records to demonstrate an issue when a controlled example is sufficient.

Stay within authorised access

A suspected weakness does not grant permission to access other users’ data or disrupt a service. Preserve the facts needed for the owner to investigate.

Prepare a clear, limited report

If you believe you have found a security issue, describe the affected page or component, the behaviour observed and the circumstances needed to reproduce it. Include the time, browser or application version and a minimal example where appropriate. Explain the potential impact as a reasoned assessment rather than a confirmed consequence if it has not been demonstrated.

Keep testing within systems and activities you are authorised to access. This page does not grant permission to probe infrastructure, bypass access controls or inspect another person's information. Do not retrieve additional confidential records merely to strengthen a report. Preserve the smallest amount of evidence needed to explain the issue and avoid distributing it through public channels.

Handle evidence carefully

Redact credentials, session tokens and personal information from screenshots or logs before sharing them. If a sensitive example is essential, agree a suitable transfer route with the responsible system owner. Record what was accessed and whether any state changed, so the owner can assess the report accurately.

For a Cobnex-delivered system, use the established security or support contact in the relevant agreement. This review website has no configured security reporting inbox or submission backend. Its contact and support forms create local documents only. Completing or downloading a form does not notify Cobnex or establish a response deadline. A live reporting policy should identify the actual monitored channel before inviting submissions.

What a useful resolution record contains

The system owner should be able to connect a report to investigation, scope assessment and corrective work. A fix may need tests for the original behaviour and related cases. If data or credentials were exposed, the response may involve actions beyond a software change, determined by the responsible organisation and its applicable obligations.

Keep communication factual and proportionate to what is known. Record the affected version, the correction, verification evidence and any remaining limitation. Coordinate publication of technical details through an agreed process rather than assuming that a fix has reached every affected environment. This resource describes reporting considerations. It does not promise a bounty, legal protection, testing authorisation or a particular response time.

Is there a published bug bounty or safe-harbour programme?

No programme is established by this page. Contact Cobnex to arrange an appropriate reporting channel before sending sensitive detail.

Read the current resource online

https://cobnex-review.rgcsekaraa.workers.dev/disclosure/