CCB SECURITY POLICY

Decided by	General Meeting
Overarching document	CCB Constitution and its amendments
Version & date	Version 1. Approved on 9 / June / 2026
Review cycle	Reviewed at least every two years, and after every recorded incident
Related documents	Information Security Standard Operating Procedures - SOP (Annex I) Operational Security Toolkit & Checklists (Annex II) Code of Conduct Travel Policy Anti-Corruption Policy Risk Management Policy Privacy Policy Cookies Policy

Content

1. Introduction

All organisations can be affected by negative events and risks during their work. Some risks such as accidents, illness, crime or extreme weather can affect Coalition Clean Baltic (CCB) and its representatives without being linked to the organisation's agenda.

Other risks arise from what we do. Our advocacy, communications, travels and partnerships can expose staff, Council members, representatives of Member Organisations, partners and beneficiaries to specific threats. We therefore need a structured way to understand, assess, reduce and respond to such risks.

This Security Policy sets out the principles that guide all our security work. The practical details - procedures, tools and step-by-step instructions - are kept in the annexes, which can be updated more easily as our context and technology change.

2. Purpose and scope

2.1 Purpose

We make security risk management an integral part of our work in order to:

- protect the life, health and rights of our staff, representatives, partners and beneficiaries;
- protect the information entrusted to us by partners, donors and members;
- protect CCB's ability to operate effectively and to maintain trust;
- comply with our legal obligations, including the EU General Data Protection Regulation (GDPR) and Swedish data protection law.

2.2 Scope

This Policy applies to the whole organisation. It is binding on:

- the Secretariat (employees and contracted staff an);
- the two Co-Chairs;
- the Council;
- the Working Area Leader(-s) and Working Group Coordinator(-s);
- representatives of Member Organisations when they act on behalf of CCB;
- external consultants, service providers and partners, to the extent agreed in their contracts or terms of engagement.

The Policy applies during planning, implementation and follow-up of activities; during paid work and voluntary commitments; during business travel; and at any other time when CCB information, equipment or property is being handled, including in private contexts.

We refer to all the people listed above collectively as "CCB representatives" throughout this Policy.

3. Principles of security risk management

Our approach is based on the following principles. They apply across all our activities and guide the more detailed rules set out in the annexes.

3.1 Life and health come first

We always put life and health ahead of business interests, assets and reputation. This applies to our own representatives and to everyone affected by our work.

3.2 Equal access to security

All representatives should have access to equal security, regardless of who they are or where they work. At the same time, we recognise that risks vary depending on roles, contexts and personal characteristics. The application of this Policy in practice may therefore differ from one person or situation to another, while keeping the overall level of protection equivalent.

3.3 Informed consent

If an activity requires an exception to our security procedures, the informed consent of the people concerned is required. Any representative may decline to take part in an activity that requires such an exception, and may withdraw at any time, without negative consequences for them.

3.4 Risk analysis and acceptable risk

Risk analysis is carried out as part of planning all activities that could expose CCB or its representatives to significant risk. The CCB Secretariat is responsible for ensuring that a risk analysis is performed and documented. Decisions about which risks are acceptable, and the reasons for those decisions, are recorded as part of risk analysis for monitoring and evaluation. Individual representatives are never expected to accept a higher level of risk than the one identified and approved for the activity.

3.5 Precautionary principles

We work on the basis of the "do no harm" principle, which is also referred to as precautionary principles. We acknowledge that some of our work, advocacy in particular, may generate friction with other actors. We always assess whether our activities could transfer risk to partners, beneficiaries or other stakeholders and vice-versa, and we take steps to ensure that such risks are known, mitigated or explicitly accepted before activities begin.

3.6 Proportionate use of resources

Security is a legitimate basis for financial and operational decisions, including when this leads to higher costs or slower delivery. Whoever plans an activity is responsible for allocating sufficient resources for it to be carried out in line with this Policy.

3.7 Transparency and confidentiality

We strive to be transparent about how security decisions are made. Any representative may request the reasons behind a security decision that affects them. CCB may, however, withhold information where sharing it would itself create a security risk. Such decisions are based on a risk assessment and are documented.

3.8 Information management

All information we handle, whether written, spoken, visual or digital, is treated according to the Information Security Standard Operating Procedures - SOP (Annex I to this Policy), the Privacy Policy, the Cookies Policy and the Code of Conduct. Information about security risks is shared internally and, where appropriate, with partners, while respecting privacy and the security of the people concerned.

3.9 Cooperation and information sharing

Good relationships with Member Organisations, partners, civil society and public authorities improve our security by increasing acceptance of our work and our understanding of the context in which we operate. We share security-relevant information with these actors when this serves our common protection. We reserve the right not to share information where doing so would expose representatives or partners.

3.10 A shared security culture

Security risk management only works if it is owned by everyone. We build and maintain a culture in which representatives can openly discuss security concerns, remind each other of good practices, and ask for help without fear of judgement.

4. Incidents, crises and response

An incident is any security-related event that affects, or could have affected, CCB representatives, partners, beneficiaries, information or assets. Examples include:

- physical threats and attacks, harassment, assault or robbery;
- digital threats and attacks, phishing, account compromise or data leaks;
- loss or theft of IT equipment;
- damage to property;
- injuries during work or travel;
- any other event that could harm the people we work with or for, or harm CCB itself.

4.1 Reporting

Anyone who is involved in or witnesses an incident report it as soon as possible. Reports are sent to the Secretariat or to the Council, using official contact channels only (according to sensitivity levels and Digital Security SOP), never through private channels such as personal email or social media.

The person reporting an incident is not responsible for managing it, but can be involved in response acitivities. Management Handling is taken over by someone who is not directly affected, in order to protect those involved and to allow for effective incident response.

4.2 Response

The CCB Secretariat coordinates the immediate response to incidents. The Co-Chairs are informed without delay of any incident that involves serious harm, significant data loss, or media or legal exposure. Where useful, external support (legal, medical, IT, communications) is engaged.

4.3 Follow-up

Each significant incident is documented and reviewed to identify lessons learned and adjustments to our procedures or tools. The CCB Secretariat prepares an annual summary of reported incidents for the Council.

4.4 Raising other concerns

In addition to security incidents, representatives may need to raise concerns about possible misconduct, breaches of CCB policies, or other irregularities. These concerns are handled under the Code of Conduct, which describes the available reporting channels and the protection from retaliation that applies to anyone who raises a concern in good faith.

5. Responsibilities

Responsibility for security at CCB follows the normal lines of governance and management. The table below summarises who does what.

General Meeting	Holds ultimate responsibility for security at CCB. Approves and amends the Security Policy and the Information Security Procedures. Ensures the Policy is made available to Member Organisations, the Council and the Secretariat.
Co-Chairs	Ensure that the Policy is implemented, known and followed across the organisation. Ensure that adequate resources are available for security work. Are informed of serious incidents without delay.
Council	Provides oversight of security risk management. Receives the annual summary of incidents. Approves changes to the Operational Security Toolkit on the recommendation of the Secretariat.
Secretariat	Carries out day-to-day security risk management: risk analyses, incident handling, training, maintenance of procedures and tools. Maintains the Operational Security Toolkit. Acts as point of contact for representatives on security matters.
Working Area Leaders and Working Group Coordinator	Ensure that security considerations are integrated into the planning and implementation of their Working Areas. Support representatives in their area in following this Policy.
Representatives of Member Organisations	When acting on behalf of CCB, apply this Policy and the Information Security Procedures to the same extent as Secretariat staff.
External IT service provider	Operates email and website services on behalf of CCB. Acts as a data processor under Article 28 GDPR and follows the terms of the Data Processing Agreement signed with CCB.
Every representative	Familiarises themselves with the Policy. Acts in line with it. Reports incidents. Contributes to the shared security culture.

5.1 Point of contact for data protection

CCB is not legally required to appoint a Data Protection Officer under Article 37 GDPR. The CCB Secretariat designates a point of contact for data protection matters from among its members. This person receives queries about personal data, supports compliance with this Policy and acts as the first interface with data subjects and, where relevant, with the Swedish data protection authority (Integritetsskyddsmyndigheten, IMY).

> ***Note:*** *If the Council decides at a later stage to formally appoint a Data Protection Officer, this section is updated accordingly.*

5.2 Exceptions

Temporary and limited exceptions to the procedures annexed to this Policy may be granted by the CCB Secretariat, after consultation with the Co-Chairs where the exception is significant. Exceptions are justified, documented and followed up.

5.3 Non-compliance

Non-compliance with this Policy may be addressed through dialogue and additional training, and, in serious or repeated cases, through disciplinary measures, termination of employment or contractual relationship, or expulsion from CCB activities, in accordance with the relevant statutes and contracts.

6. Review of this Policy

This Policy is reviewed at least every two years, and earlier if a significant change in our context, legal environment or organisation makes it necessary. Additionally, it is reviewed after each documented incident (together with all relevant security procedures and SOPs.

Any representative may suggest revisions, additions or new related documents. Suggestions are addressed to the Council. If the Council considers the suggestion appropriate, it is brought to the next General Meeting for decision.

The Information Security Procedures are reviewed at least once a year by the Secretariat and approved by the General Meeting. The Operational Security Toolkit is maintained by the Secretariat and updated whenever needed, with notification to the Council.

— End of Security Policy —

CCB Information Security Standard Operating Procedures (SOP)

Annex to the CCB Security Policy

Decided by	General Meeting
Maintained by	Secretariat
Version & date	Version 1. Approved on date / month / 2026
Review cycle	Reviewed at least once a year, or earlier if needed
Related document	Security Policy Operational Security Toolkit – Annex II (maintained by the Secretariat, updated as needed)

Content

1. Introduction

The CCB Information Security Standard Operating Procedures (SOP) translates the principles of the CCB Security Policy into practical rules for handling information. They apply to all CCB representatives, as defined in the Security Policy, and to all information we create, receive, store, share or destroy in the course of our work, regardless of whether it is on paper, in digital formats, in spoken form, on a screen, in an audio recording or a photograph.

Responsible for enabling this work is the CCB Executive Secretary. Everyone shall read and follow the SOP when joining the organisation.

Where these SOP set a requirement (for example, "all devices must use full-disk encryption"), the requirement is binding. The specific tools and step-by-step instructions for meeting these requirements are described in the Operational Security Toolkit, which is updated by the CCB Secretariat as our tools change.

> ***Note:*** *If you are unsure how to apply a rule to a specific situation, ask the CCB Secretariat.*

2. Why we protect information

We protect information for several reasons:

- to protect our staff and representatives from unnecessary risk;
- to protect our partners and beneficiaries from repression or harm;
- to protect rights holders and individuals whose data we hold;
- to comply with the GDPR and other legal requirements;
- to sustain our ability to work in sensitive locations and on sensitive topics.

3. The three goals: confidentiality, integrity, availability

When handling information, we aim to protect three things at the same time. This model is internationally known as the "CIA triad":

- **Confidentiality.** The information is only accessible to people who are authorised to see it.
- **Integrity.** The information is correct, complete, up to date and has not been changed without authorisation.
- **Availability.** The information is accessible to authorised users when they need it.

***Note:** "CIA triad" is the standard name in information security.*

4. Classifying information

We classify our documents and information into three levels. Classification determines how a piece of information may be stored, shared and discussed.

Level	Meaning	Examples
GREEN	Can be shared publicly without harm.	Published reports, public communications, our website content, public position papers.
YELLOW	Should not be shared publicly, but can be shared internally within CCB without additional protection.	Internal drafts, working documents, internal meeting minutes, day-to-day correspondence with partners, project budgets.
RED	Sensitive. Could harm individuals or the organisation if disclosed. Shared only on a need-to-know basis with additional protection.	Personal data (addresses, ID numbers, health information), salary information, bank details, passwords, contracts, personnel records, sensitive partner or beneficiary information, incident reports.

4.1 Who classifies

The information owner, usually the person who creates the document or receives it first, assigns the classification. Anyone in CCB can raise the level of a document to a more restrictive one. Only the information owner, or their manager, can lower it.

4.2 Classification in practice

- A document is classified based on its most sensitive content, even if the rest is non-sensitive.
- Drafts may need a higher classification than the final version, because they often contain unverified or work-in-progress material.
- Where possible, mark the classification in the file name (e.g. "1-green", "2-yellow", "3-red") so it is immediately visible.
- When in doubt, classify higher rather than lower. You can always lower it later.

4.3 Special categories

Some information is always treated as RED, regardless of context. This includes:

- personal data of staff, members, partners or beneficiaries (addresses, phone numbers, ID numbers, health data, etc.);
- financial information such as bank accounts and payment details;
- credentials (user IDs, passwords, PINs, recovery codes);
- legal documents, contracts and personnel records;
- incident reports (initially, the level may be lowered later, on a case-by-case basis).

5. Access to information

Access is granted on a need-to-know basis. The information owner decides who has access, in consultation with their manager when needed.

5.1 Granting access

- Access is given to people who need the information to do their work.
- Access is reviewed regularly, and at the latest when a person changes role or leaves CCB.
- Where the same information needs to be available in different contexts (e.g. public and internal), we publish different versions instead of widening access.

5.2 External consultants and partners

External consultants and partners may only receive YELLOW or RED information after they have signed a confidentiality agreement, or after a written commitment is in place that covers the handling of the information.

5.3 Off-boarding

When a representative ends their role at CCB, the CCB Secretariat ensures that, within two weeks (or within another short period of time agreed with the CCB Executive Secretary):

- an out-of-office reply is set on their CCB email;
- relevant work files and folders are handed over;
- their accounts on CCB systems (email, cloud storage, messaging groups, password manager, tools) are closed or transferred;
- any shared passwords they had access to are changed;
- they are removed from internal mailing lists and groups.

6. Devices

6.1 Work devices

We aim to keep the number of devices that hold CCB information small. Each representative who needs digital access for their work uses, as a rule, one computer (laptop or desktop) and one smartphone for CCB activities.

6.2 Personal devices

CCB does not provide devices to all categories of representatives. Personal devices are therefore in regular use, in particular by Council members, Co-Chairs, Working Area Leaders, and representatives of Member Organisations.

When personal devices are used for CCB work, the following requirements apply:

- the device is protected by a screen lock (PIN, passphrase or biometrics, see 6.3);
- full-disk encryption is enabled (this is the default on recent iPhones, iPads, Android phones, and on macOS and Windows when set up correctly);

- the operating system and applications are kept up to date;c
- CCB information stored locally is removed once it is no longer needed, and is not shared with non-CCB users of the device (for example, family members).

6.3 Screen lock and biometrics

All devices used for CCB work must be locked with a PIN, passphrase or biometric authentication when not in use. As a default, biometric authentication (fingerprint or face) combined with a strong PIN or passphrase as fallback is acceptable and often more secure than a short PIN alone.

> ***Note:*** *When travelling to a country where searches at borders are a realistic concern, or in any situation where coerced unlocking is plausible, switch to PIN/passphrase-only and turn devices off before crossing controls. Full-disk encryption only protects you when the device is fully powered off. See section 9 on travel.*

6.4 Lost or stolen devices

A lost or stolen device that contains CCB information, or has access to CCB accounts, is treated as a security incident. Report it to the CCB Secretariat as soon as possible. The CCB Secretariat coordinates the response, which typically includes remote wipe, password changes and a review of what information was on the device.

7. Accounts and passwords

7.1 Two-factor authentication<

All accounts used for CCB work - email, cloud storage, messaging, password manager, tools, social media accounts of the organisation - must have two-factor authentication enabled.

The CCB Operational Security Toolkit lists which app or method to use for each service.

7.2 Password manager

CCB uses a password manager to store, generate and share passwords. Staff working at the CCB Secretariat has access to the organization’s account. The specific product currently in use is listed in the CCB Operational Security Toolkit.

7.3 Password quality

Passwords must be:

- **long:** at least 15 characters (including at least one upper and lower case letter, numbers), or a passphrase of at least 6 random words separated by spaces;
- **unique:** never reused across services;
- **generated, not invented:** use the password manager to generate new passwords.

7.4 Sharing passwords

Avoid sharing passwords when possible: most services allow granting access without sharing credentials. When sharing is necessary, use the password manager’s sharing feature or an end-to-end encrypted channel. Never send passwords by regular email, SMS or social media.

8. Handling information

8.1 Storage

Information is stored in the systems approved for its classification level. The list of approved systems and their intended use is kept in the CCB Operational Security Toolkit.

- GREEN information may be stored in any CCB system, including those used for public publication.
- YELLOW information is stored in our internal collaboration and storage systems, with access limited to CCB representatives.
- RED information is stored in systems that support strong access controls, and is shared only with the specific people who need it.

8.2 Sharing

Before sharing information, check:

- that you are allowed to share it;
- that the recipient needs it for their work;
- that the recipient will handle it according to CCB standards;
- that the channel you are using is appropriate for the classification level.

For RED information, use end-to-end encrypted channels. For sharing of files outside CCB, prefer encrypted file links with limited validity over email attachments. The CCB Operational Security Toolkit describes the current recommended methods.

8.3 Email

- Email is suitable for GREEN information and, with care, for YELLOW information.
- Do not put RED information in the subject line, the "to" or "from" fields, or in unencrypted attachments.
- **Do not forward CCB work emails to personal addresses, or to email accounts at other organisations. This is both a GDPR concern and a security risk.**
- Be alert to phishing. If a message is unexpected, asks you to click a link or open a file urgently, or comes from a sender you cannot verify, pause and check through another channel.

8.4 Instant messaging and voice

For internal team communication and for contacts with partners on sensitive topics, use the end-to-end encrypted messaging tools listed in the CCB Operational Security Toolkit. Avoid carrying out sensitive conversations on SMS or on platforms that are not end-to-end encrypted.

Voice and video calls follow the same rule: sensitive conversations take place on tools that offer end-to-end encryption. Where commercial platforms are used (for instance because a partner requests it), enable the available security options and avoid recording.

8.5 Spoken information

- Be aware of who can hear you. Public transport, cafés and open offices are not appropriate places to discuss RED information.
- Speaking in a foreign language does not make a conversation private.
- Phone calls on the ordinary phone network are not secure against interception Be especially careful when discussing personal information about colleagues, partners or beneficiaries.

8.6 Printed documents

- GREEN printed documents can be stored openly and taken outside the office.
- YELLOW printed documents are kept in the office, in a drawer or shelf when not in use.

- RED printed documents are kept in a locked drawer or safe and do not leave the office, unless this is specifically authorised. When a safe is shared, a list of people with access is maintained.
- Documents that are no longer needed are shredded, not put in the regular paper bin.

8.7 USB sticks and external drives

- Do not plug in USB sticks or drives whose origin you do not know.
- If you need to carry CCB information on external media, encrypt it.
- Once the transfer is done, securely erase the data from the external media.
- Do not lend external media used for CCB work to people outside the organisation.

8.8 Backups

The systems approved by CCB for storing work data perform their own backups. Personal copies on USB sticks or local drives are not a substitute for these systems, and create additional risk. If you have a specific need to back up data outside CCB systems, discuss it with the CCB Secretariat first.

8.9 Secure deletion

When deleting RED information, simply moving the file to the trash is not enough. The CCB Operational Security Toolkit describes how to delete data securely on the systems we use.

9. Information security while travelling

When travelling for CCB, take the following precautions:

- Before you leave, take only the data you actually need. Where possible, leave RED information at home and access it remotely once you are at a safe destination.
- Use the CCB-approved VPN on all networks outside home or CCB-office (hotels, cafés, airports, conference venues).
- Keep full-disk encryption enabled on all devices. Turn devices off, not just sleep mode, when crossing borders or going through security controls.
- In contexts where coerced unlocking is a realistic concern, switch from biometric unlock to PIN/passphrase before travelling.
- Keep devices on your person when possible. Do not leave them in hotel rooms without protection.
- Clear browser cache, cookies and saved passwords after using a public or shared computer.
- Be aware of local laws on encryption, VPN use and content.

A travel checklist is included in the CCB Operational Security Toolkit and complements the CCB Travel Policy.

10. Working from the office, home or public spaces

10.1 At the office

- Lock or turn off your screen when leaving your desk.
- Do not leave RED documents visible when non-CCB visitors are present.
- Visitors are not left unattended in spaces where CCB information is accessible.

10.2 At home

- Always use the CCB-endorsed VPN, when not at home or in the CCB-office or when not using your phone's personal hotspot (be aware, that VPNs on the phone do not protect devices, which are connected to the hotspot).
- Keep printouts and external media in a locked space when you are away.
- Be aware of smart speakers, cameras and other connected devices in the room where you work.
- Other household members do not use CCB accounts or devices.

10.3 In public spaces

- Use the privacy screen protector, or sit so that your screen is not visible to others.
- Always use the CCB-endorsed VPN, when not at home or in the CCB-office or when not using your phone's personal hotspot (be aware, that VPNs on the phone do not protect devices, which are connected to the hotspot).
- Avoid discussing or displaying RED information. Be aware of CCTV cameras around you!

11. Public communication and social media

All public posts about YELLOW or RED projects are coordinated with the CCB Communication Officer and signed off by the relevant Working Area Leader or the CCB Secretariat.

When posting publicly:

- Check the background of any photo for sensitive details (post-it notes, lists of contacts, screens, badges).
- Make sure you have the consent of people in photos or videos.
- Avoid revealing personally identifiable information about partners, especially those in sensitive contexts.
- When in doubt, do not publish.

12. Communicating with at-risk partners and beneficiaries

Some of our partners and beneficiaries face elevated security risks. When working with them:

- Follow their lead. They know their context best. Ideally it meets or exceeds the CCB-standards.
- Offer them communication channel options. Be ready to use end-to-end encrypted tools, non-CCB-branded contact details, or other measures if these reduce their risk.
- Where their preferred channel would expose them or CCB to unacceptable risk, propose alternatives. If no acceptable common ground exists, this is itself a security decision to be discussed with the CCB Secretariat.
- Document the secure communication agreement with each partner.

13. Artificial intelligence (AI) and generative tools

Generative AI tools can be useful tools, but they also create specific information-security risks. In particular:

- Your requests, prompts, and data are collected and stored and can be linked to your identity or identities;
    - This data can be handed over to authorities upon legal requests;

- AIs can use the data we insert to train future models;
- Third parties may have access to data without authorization (e.g. through security vulnerabilities or cyber and phishing attacks);
- Environmental impact of generative AI use (energy and water consumption);
- Dependency of workflow and capacities on an external service provider.

13.1 What you can do

Preparation:

- Use local AIs either on own laptop or specific organizational device;
  - guardrail strictly the access of the AI app to the data it needs to process;
- Use a VPN to connect to online AI services and use anonymous accounts (non-CCB email addresses);
- Select AIs that certify not to use and store data;
- Select AIs outside US, Chinese, Russian jurisdiction;
- Make your use of AIs transparent to the CCB Secretariat and to colleagues in your Working Area when relevant.

Usage:

- If possible, try to use services, which do not need a sign-on.
- If you need to sign-on, sign up with an anonymous or functional e-mail account, not pointing to your organization or identity.
- If it is unavoidable the need to use the paid version of commercial platforms create a protocol to protect identity when paying (e.g., disposable debit cards).
- Use of AI tools for GREEN content is accepted: drafting public communications, brainstorming, summarising public material, learning about a topic.
- You may use AI tools to improve language and style of text you have written yourself (avoiding sensitive data).
- Create a criteria list, of what content and words might be sensitive information not to share with the AI services, confirm this list with management.
- Disclose the use of AI when this is relevant for the recipient (for example, in academic or formal contexts).

Follow-up:

- Copy all necessary AI-replies to your external documents or alike and then delete them from your history of the AI-service. If it's a service storing personal data, be aware this does not mean they delete them from their databases.

13.2 What you must not do

- Do not paste RED information into AI tools. This includes personal data, partner names where they could be at risk, internal financial details, passwords and credentials.
- Do not paste YELLOW information into AI tools. Exceptions can only be granted by the CCB Secretariat management (minimum criteria: "no training" or enterprise-grade setting).
- Do not use AI tools to make decisions about people (e.g. about partners, applicants, beneficiaries).
- Do not assume AI output is accurate. Verify facts, names, citations and figures before using them in CCB material.

13.3 Account setup

Where agreed upon AI tools are used regularly for CCB work, the CCB Secretariat sets up dedicated accounts and configures privacy settings. Personal free-tier accounts are not to be used.

> ***Note:*** *A more detailed AI guideline may be developed with input from a security consultant and integrated into the CCB Operational Security Toolkit when ready.*

14. Reporting incidents

Section 4 of the Security Policy describes how incidents are reported and handled. In summary:

- Report as soon as possible to the CCB Secretariat or, if not possible, to a Co-Chair or Council member, through official channels only.
- Do not try to handle a serious incident on your own.
- Keep notes of what happened, when, and who is involved.
- If a personal data breach is involved, it may need to be notified to the Swedish data protection authority (IMY) within 72 hours. This is the responsibility of the CCB Secretariat, but timely reporting from your side makes this possible.

15. Maintaining a security culture

These SOP only work if they are used. The CCB Secretariat:

- organises onboarding briefings for new representatives;
- offers refresher sessions at least once a year;
- shares relevant news, examples and small exercises with the team;
- makes time for open conversations about what works and what does not.

Every representative is encouraged to ask questions, propose improvements, and remind colleagues, including senior ones, when a security practice is being overlooked. Doing so is a contribution to the organisation, not a complaint.

16. Review of these Procedures

These SOP are reviewed at least once a year by the CCB Secretariat, with input from the Council and the Co-Chairs. Changes are submitted to the General Meeting for approval. The CCB Operational Security Toolkit, which accompanies these Procedures, is updated more frequently by the CCB Secretariat as tools and threats evolve, and the Council is notified of significant changes.

— End of Information Security Procedures —

CCB Operational Security Toolkit

Practical guide to the tools, checklists and routines used at CCB Secretariat

Maintained by	CCB Secretariat
Version & date	Version 1. Approved on date / month / 2026
Update cycle	Updated as needed by the CCB Secretariat. Significant changes are notified to the Council.
Related documents	CCB Security Policy CCB Information Security Standard Operating Procedures (SOP) – Annex I

Content

1. How to use this toolkit

This Toolkit is the practical companion to the CCB Security Policy and the CCB Information Security Standard Operating Procedures (SOP). It lists the tools we currently use, gives short instructions for the most common tasks, and provides checklists for routine situations.

Unlike the Policy and the Procedures, the Toolkit changes frequently. New tools may be added, old ones removed, instructions refined. The CCB Secretariat keeps it up to date and notifies the Council of significant changes.

If you find an instruction that no longer works, or a tool that has changed, inform the CCB Secretariat so the Toolkit can be corrected.

2. Tools currently in use at CCB

The table below lists the tools currently approved for CCB work, the purpose they serve, and the most important things to know about each. Detailed setup instructions follow in section 3.

Purpose	Tool	Notes
Shared documents	Dropbox, CryptPad, Google Workspace	2FA mandatory.
Email	Delta	CCB email accounts (@ccb.se) and website are operated by our external IT service provider.
Instant messaging	Signal	For team chat and for sensitive conversations with partners. Use Registration Lock (PIN) and usernames (instead of your phone number).
Video meetings	Zoom (Signal for sensitive calls)	For internal and external meetings. Use end-to-end encryption where available, waiting rooms, and avoid recording sensitive meetings.
Collaborative editing of sensitive docs	CryptPad, Nextcloud	For drafting and sharing documents that should not pass through commercial cloud platforms. Use password-protected links.
Password manager	Bitwarden	One shared account. Strong master password and 2FA mandatory.
Two-factor authentication	FreeOTP (or built-in authenticator)	Used for accounts that support time-based one-time codes (TOTP). Backup codes stored in Bitwarden.

Note: *If a partner or Member Organisation proposes a different tool for a specific exchange, discuss it with the CCB Secretariat before agreeing. Some commercial tools have known weaknesses or are inappropriate for sensitive content.*

3. Setting up the basics

Every representative who works regularly on CCB matters should complete the steps in this section. The CCB Secretariat supports onboarding and is available to help.

3.1 Strong screen lock on every device

1. Set a screen lock on every device you use for CCB work: laptop, desktop, smartphone, tablet.
2. Use a PIN of at least 6 digits, a passphrase, or biometric unlock combined with a strong PIN as fallback.
3. Set the device to lock automatically after a short period of inactivity (one to five minutes).

3.2 Full-disk encryption

Full-disk encryption protects the content of a device when it is turned off. On modern devices it is usually on by default, but check:

- iPhone / iPad: encryption is automatic once a passcode is set.
- Android: encryption is automatic on recent devices; on older ones it may need to be enabled in Settings.
- macOS: enable FileVault in System Settings > Privacy & Security.
- Windows: enable BitLocker (Pro / Enterprise editions) or Device Encryption (Home edition) in Settings > Privacy & Security.
- Linux: enable full-disk encryption during installation.

Note: *Encryption only protects you when the device is fully powered off. A locked but running device can still be attacked. When you are concerned about device seizure, shut down, do not just lock.*

3.3 Two-factor authentication (2FA)

1. In each CCB account, find the security settings.
2. Enable two-factor authentication.
3. Where possible, use an authenticator app (FreeOTP or the built-in authenticator on your phone), not SMS.
4. Save the recovery codes provided during setup in your Bitwarden vault.
5. For day-to-day and more secure use (against phishing), set up a Passkey for each account in addition to 2FA with authenticator app). Use the Passkey option for daily access.

3.4 Bitwarden password manager

1. The CCB Secretariat shares a Bitwarden account with staff members.
2. Choose a strong master password (long passphrase) that you do not use anywhere else. Write it down once and keep it in a physically safe place until you are sure you remember it.
3. Enable 2FA on the Bitwarden account itself and Passkey use.
4. Install the Bitwarden app on your phone and the browser extension on your work browser.

5. Move existing passwords into Bitwarden within four weeks of onboarding Bitwarden and delete them from your previous locations (eg. Browsers). Replace weak or reused ones with generated passwords.

3.5 Signal

1. Install Signal from the official app store on your phone.
2. Set a Signal PIN and enable Registration Lock (Settings > Account > Registration Lock).
3. Enable disappearing messages by default for new conversations (Settings > Privacy > Default timer on maximum 4 weeks, depending on risk assessment)
4. Enable usernames and hide your phone number.

3.6 Zoom

- Sign in to the CCB account.
- In your account settings, enable "Require encryption for third-party endpoints" and "Allow use of end-to-end encryption" for sensitive meetings.
- Use waiting rooms for external meetings.
- Do not record meetings unless this is necessary and consented to by all participants. Download all recordings after the Zoom-meeting and delete them from Zoom. Recordings of YELLOW or RED content are stored in CCB-approved systems, not on personal computers.

3.7 CryptPad

- Create an account with 2-factor-authentication at cryptpad.fr (or the instance specified by the CCB Secretariat) and save the credentials in Bitwarden.
- For sensitive documents, use the password protection feature in the "Access" menu before sharing the link.
- Move documents out of CryptPad once they are no longer being worked on. Delete pads that are no longer needed.

4. How-to guides for common tasks

4.1 Sharing a sensitive file with a colleague

1. Check the classification of the file. For RED content, prefer CryptPad or a 2FA-protected shared drive, not email attachments. Alternatively, via Signal.
2. Tell the colleague through a separate channel (Signal, call) that the file is coming. This helps them spot phishing if a similar-looking message arrives from elsewhere.
3. Share the file with the specific person, not a broad link.
4. Where the platform allows it, set an expiry date on the link or access.

4.2 Sharing a password with a colleague

1. Open Bitwarden.
2. Use the sharing feature for the specific item or collection.
3. Do not paste the password into email, Signal, SMS or any other channel.

4.3 Recognising a phishing attempt

Warning signs:

- Urgency or fear in the message ("your account will be closed in 24 hours").
- A sender address that looks similar to a real one but with small differences.
- A link that, when you hover over it, points to a different address from the visible text.
- Unexpected attachments, especially .zip, .exe, .iso, or Office files with macros.

- Requests for credentials, codes or sensitive information.

If you are unsure: do not click. Forward the message to the CCB Secretariat, who can check and respond. It is always better to ask.

4.4 Reporting a security incident

1. Notify the CCB Secretariat as soon as possible, through Signal, phone or in person, not through the system you suspect is compromised.
2. If you cannot reach the CCB Secretariat, contact a Co-Chair or Council member through a secure channel.
3. Write down what happened, when, and which systems or information may be involved.
4. Do not try to investigate or fix the incident on your own.
5. Do not delete anything that might be evidence (suspicious emails, files, screenshots).
6. If you fear, your device is affected, take it offline and report the incident from a different device.

4.5 Using AI tools safely

- Before pasting anything into an AI tool, ask: would I be comfortable if this text appeared in a public dataset?
- For RED information, the answer is no. Do not use AI tools.
- For YELLOW information, check with the CCB Secretariat which tool is approved.
- For drafting GREEN content, AI tools can be useful, always verify facts and figures before publishing.
- Use a VPN and don't use AIs from USA, China and Russia.
- Check the SOP for more detailed guidance on usage.

5. Checklists

These checklists are short reminders of the steps to take in specific situations. Keep them at hand.

5.1 Creating or storing information

- ☐ Have I assigned a classification (green, yellow, red)?
- ☐ Am I storing this in the right system for its classification level?
- ☐ Have I given access only to the people who need it?
- ☐ Is the file name clear enough to be found later? Does it include the classification?

5.2 Sharing information

- ☐ Am I allowed to share this?
- ☐ Does the recipient need it to do their work?
- ☐ Is the recipient able and willing to handle it according to our standards?
- ☐ Is the channel I am using appropriate for the classification?
- ☐ Have I let the recipient know to expect the file or message?

5.3 Spoken conversations about CCB work

- ☐ Is the space I am in private enough for what I want to discuss?
- ☐ Could the conversation be overheard, recorded, or intercepted?
- ☐ Am I about to mention names, locations or details that should stay confidential?
- ☐ Would it be better to move this conversation to a Signal message or a secure call?

5.4 Hard copies and printed documents

- ☐ Classification clear on the document? (Green / Yellow / Red)
- ☐ Stored in an appropriate place, open shelf (Green), drawer (Yellow), locked space (Red)?
- ☐ Is the list of who has access to shared safes / cabinets up to date?
- ☐ When no longer needed: shredded, not put in the regular bin?

5.5 Before a work trip

- ☐ Travel risk briefly assessed (destination, context, sensitivities)?
- ☐ Only the data needed for the trip is on the devices?
- ☐ VPN installed and tested?
- ☐ Full-disk encryption confirmed on all devices?
- ☐ Screen lock set to a short timeout?
- ☐ In sensitive contexts: biometric unlock turned off in favour of PIN / passphrase?
- ☐ Emergency contacts noted (CCB Secretariat, Co-Chairs)?
- ☐ Travel Policy and SOP reviewed?

5.6 After a work trip

- ☐ Browser cache, cookies and saved passwords cleared if a public computer was used?
- ☐ Devices checked for anything unusual?
- ☐ Any incident or near-miss reported to the CCB Secretariat, even if no harm occurred?

5.7 Onboarding of a new representative

- ☐ Security Policy and SOP shared and explained.
- ☐ CCB email account created.
- ☐ Bitwarden account created and shared collections assigned.
- ☐ Signal contact added.
- ☐ Zoom and CryptPad accounts created where needed.
- ☐ Short onboarding session held (live or recorded) covering the basics.
- ☐ 2FA + Passkeys enabled on all CCB accounts.
- ☐ Full-disk encryption confirmed on the devices used for CCB work. For use of computers for other purpose then CCB: Separate user profile created.

5.8 Off-boarding

- ☐ Files and folders handed over.
- ☐ Out-of-office reply set on the CCB email.
- ☐ CCB email and cloud account closed or transferred.
- ☐ Removed from Signal groups, mailing lists, shared CryptPad folders.
- ☐ Bitwarden access revoked; passwords of shared accounts changed.
- ☐ Access to any other CCB systems reviewed and removed.
- ☐ Confirmation logged what off-boarding steps are done and that off-boarding is complete (target: within two weeks).

— End of Operational Security Toolkit —