---

eMail to the Collaboration:

Subject: Collaborating Online: Data Privacy and Security

Dear all

As we continue to **collaborate and share our work**, it is important to remember the **balance between openness and data privacy and security**. We are all about making our resources and information accessible without needing special accounts. However, this commitment comes with a **responsibility to protect our shared data**. Consequently, to address concerns raised on data privacy and security, the spokespersons asked us, the Software & Computing coordinators, to prepare guidelines for our daily work in ePIC.

To support the balance between openness and data privacy and security, we **advise limiting editing access to shared resources and documents**, **using secure platforms**, and **sharing links to our information wisely**. We have prepared a limited set of guidelines that are accessible on the web: **https://eic.github.io/policies/data_privacy_collaboration.html**

We all play a part in keeping our collaborative efforts productive and secure. Thanks for doing your bit!

Best regards,

Guidelines to Be Posted on the Web:

We all play a part in keeping our collaborative efforts productive and secure. Thanks for doing your bit!

Limit editing access:

- **While using Google Workspace for shared documents, presentations, and spreadsheets**: Depending on the share settings, anonymous or unknown people can comment or edit. This exposes the documents to risks such as vandalism. These risks can be avoided by explicitly giving comment-access or write-access to people who need to edit, and asking others to request access. If a document doesn't need edits, make it read-only for those logged in. Furthermore, do not share links to entire Google Drive

folders, but rather explicitly grant access to collaborator's Google accounts, similar to write/comment access for shared documents.
- Some of our **mailing lists** have archives and some of these archives are publicly accessible. If you are the owner of a mailing list, take a moment and adjust the privacy settings. Note that email archives can contain sensitive information that should not be exposed to the open internet.
- To ensure every account on **GitHub** and **Mattermost** corresponds to a real person that could reasonably belong to an ePIC collaborator (in the absence of a formal memberlist), we enhanced our account policy.
    - GitHub users must include their full name and current affiliation on their GitHub profile.
    - Mattermost users must include their full name and valid email address in their profile.

Use secure platforms:
- When we are working on documents together, using platforms like GitHub, HedgeDoc, or Overleaf is a smart move. These sites make sure everyone logs in first, which helps keep our work secure.

Share links wisely:
- Be mindful about where you are sharing links to our internal documents. Public links can get out of hand, so let's aim to share smartly and keep our stuff safe. For live notes during meetings, either use secure platforms or distribute the write-enabled link exclusively within the Zoom chat. Also keep in mind that some information (such as vendor-specific performance) could be sensitive information, which should never be publicly posted or linked.

We all play a part in keeping our collaborative efforts productive and secure. Thanks for doing your bit!

Additional Actions:

- **GitHub accounts**: SCC responsibility
    - **Important context**:
        - EIC GitHub is not exclusive to ePIC but rather all of the EIC community.
        - In practice, we have the following requirement: we will give access to anyone who's an ePIC or EICUG member, or anyone who is *"sponsored"* (vouched for) by an ePIC or EICUG member.
        - There are groups for write access to repositories, e.g., ePIC Devs for the ePIC repositories with currently 167 members.
    - Institute real name and affiliation policy. Mentioned in policy.

    - Require team-based permissions for repositories (individual admin/maintain permissions subject to removal without notice).
    - Regular purging of external collaborators (and sending an invitation to join where appropriate).
    - Require 2FA for anyone to hold admin and maintain roles.
    - Stored trigger tokens and secrets:
        - Keep inventory and rotate regularly.
- **Mattermost**: SCC responsibility
    - Institute real name and email address policy. Mentioned in policy.
    - Regular automatic purging of failing email addresses.
    - Transition to requiring GitHub account credentials for new users.
- **Indico**:
    - Explore whether it is possible to restrict access to the Zoom information in the event description to only users who are logged in, while also ensuring that any Zoom link remains usable.
    - Related to that: Explore whether it is possible to restrict top-level event description visible to logged in users only.
    - Restrict access to subcategories to a more limited number of users (i.e. move ePIC up in the hierarchy and have only a handful of admins).
- **Services**:
    - Annual audit of inactive accounts.