Routine maintenance of ScHARR resources on University Departmental Storage (typically mapped as the “X: drive”) v2.0

This version (v2.0) approved IG Committee 5 May 2022

Overview

In order to ensure ScHARR resources on University Departmental Storage are being appropriately managed, and Information Asset Owners (IAOs) are fulfilling their obligations, routine checks are carried out. Routine checking is important to ensure access is kept up to date; data in folders is appropriately archived and deleted; and responsibility and ownership is maintained for University data assets.

Process

Selecting a folder *for checking*

A folder check is generally triggered by a change request, logging of an incident, or users with expired training, i.e. the following would likely trigger a folder access check:

- A change of IAO
- Significant changes to structure or access
- The folder has an ‘external’ user with expired training (this check involves working though the list of folders manually)
- A specific request (e.g. from IG Committee)
- Suspicion that folder isn’t being managed very well (e.g. an incident has been logged)
- More than 10 years have elapsed since folder creation (where it is possible to work through this list)

Carrying out the folder check

- ScHARR-DS sends the information about the folder to the IAO via email, with any relevant additional details or requests. The IAO is asked to respond to the email as appropriate, depending on the nature of the check. See Appendix A: Example first email
- If there is no response after one week, ScHARR-DS will send a follow-up email as a reminder. See Appendix B: Example second email
- If there is no response after a further week, ScHARR-DS will send a second follow-up email with a reminder that folder checks are an audit requirement, cc’ing in any Deputy IAOs, and reiterating the specific information required. See Appendix C: Example third email
- Finally, if there is still no response one week later (i.e. over a month after the initial email), ScHARR-DS will
    - remove access for users with expired training records as a precautionary measure

- raise an IG incident
- email the IAOs. See Appendix D: Example final email

Appendix A: Example first email

This is a routine folder check for [folder name]

Can you confirm that we have the details correct and that the people who have access still need access?

Can you confirm if any of the control folders contain risk-bearing data? If any users do not have up-to-date InfoSec Training records they will be contacted individually, but if they have access to risk-bearing data then we'll need to temporarily put their access on hold until they're back up-to-date.

(if applicable)
We also need a short description of the folder for the audit list, please.

(if applicable)
You don't have access to all of the folders - that's not a problem, but you just need to be aware that as IAO you are still responsible for them. If you need access, please let us know.

(if applicable)
Could you give us an estimated expiry date? This will flag up the folder for review, and should take into account any data sharing agreements or other contractual obligations. Note that we'll always contact you before we delete or archive anything.

If you need to make any other changes, please let me know.

Folder details:
Folder Number: X0000A
Folder Name: [e.g. PR_xxxxxx]
Area: [e.g. ScHARR]
Filepath: [e.g. X:\ScHARR\PR_xxxxxx]
Description: xxxxxx
-
Responsibility
Information Asset Owner: [username - name]
Deputy IAO 1: [username - name]
Deputy IAO 2: [username - name]
Deputy IAO 3: [username - name]
-
Status
Status: (Active / Deleted / Archived etc)
Expiry: [date]
Created: [job ref]
Check: [job ref(s)]
-

Control Folders
Control Folder 1: xxxxxx (Active / Deleted / Archived etc)
[list of users with access]

Control Folder 2: yyyyyy (Active / Deleted / Archived etc)
[list of users with access]

Control Folder 3: zzzzzz (Active / Deleted / Archived etc)
[list of users with access]

Appendix B: Example second email

I emailed you on [date] about [folder name] but I haven't heard back from you yet, so this is a follow-up to make sure it doesn't get missed.
You can click the Self-Service link at the bottom of this email to see the message if you no longer have the original email.

Appendix C: Example third email

I'm following up about the check on [folder name] again. This is now the third email since this check was initiated, and as folder checks are an audit requirement, if I don’t get a response I'll need to:

1 - Remove access for all users who do not have an up-to-date Information Security Training record
2 - Record a failure to respond against the folder check
3 - Record an IG incident for referral to the IG Committee

Obviously this creates additional work for us all, and I realise that you are already busy so if we can get a response this week I'll be able to close the job before the above steps must be carried out.

From this morning's report, the current users with access are:
[list of current users]

Appendix D: Example final email

Having still not received an answer regarding access to the check on [folder name], as advised in my previous email of [date] I've been obliged to take the following action:

The following access changes have been made:
[list of access changes]

The folder check has been noted as 'Failure to respond'

An IG incident has been recorded (IGxxxxxx). You may receive a follow-up from the IG Committee in due course if further investigation is required.

Please let me know if you have any questions.

Version control

Version	Effective Date	Summary of changes
1.0	27/0342021	n/a first version
2.0		Changed ‘folder administrators’ to ‘IAOs’, made it clear that the email templates are examples, changed the follow up period to 1 week rather than 2 weeks. Email templates revised.