UNIVERSITY OF THE WEST of SCOTLAND

UWS

Guidance Document for Staff – MS Teams

Version1.2 – November 2023

Policy Statement Author – IT Security and Customer Support Manager

Procedure Owner – Director of Information Services

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version – Version 1.2 – November 2023

Changes and Reason for Changes – New Guidance

DOCTRINA PROSPERITAS

Purpose

The purpose of this document is to enhance the security posture for all service users at UWS. Please take the time to read these guidance notes and familiarise yourself with best practices around Team management. Note that if guidance is not followed Teams may be deleted without notice where there is a perceived risk identified.

Related Documents

- Acceptable Use Statement MS Teams

Do

- Give Teams appropriate names to make them identifiable. Teams labelled as 'Test' or without a descriptive title will be deleted.
- Be vigilant for suspicious 'guests' in meetings. Is there anyone on the meeting call you wouldn't expect.?
- Ensure a Team has more than 1 'Owner' role. Where there are not at least 2 owners assigned the role of 'owner' a member of the Team will be automatically elevated to this role.
- Have a portrait photograph as your Teams profile picture.
- Regularly (suggested monthly) review of Team membership to ensure appropriate removal of members when they no longer require access and that the site is deleted at the appropriate time.
- Take care when adding files to Team Groups as the entire Team membership will see. Only add Team members who are permitted access to content (Files/conversations etc.).
- Only add data content to a team if the entire membership should have access privileges.
- Delete Teams as soon as they are no longer required. Owners of Teams not used for 12 months will be emailed to advise that it is intended to delete the Team and given the option to justify the extension of use.
- Ensure created Teams are marked as 'Private'. Anyone can access a public Team without an invite.
- When creating a team, check whether it is appropriate to re-use an existing Team to avoid duplication.
- Keep Team content clearly labelled, current and well structured.
- Refer to Data Handling and Classification Protocol if you are unsure on what should be shared with a Team.

Don't

- Create a Team name which uses offensive language or terms. These Teams will be deleted without warning and disciplinary action may be taken.
- Add external members to Teams. Requests for externals to be added must be logged with IT Services via a Change Request in TOPdesk. Failure to do this may result in disciplinary procedure.
- Download Teams content to a 3rd party app/storage location.
- Change setting for a team from 'Private' to 'Public' without approval (Dean or Director and IT).
- Rename a Team without informing membership.
- Add files/attachments to Teams chats. This makes them difficult to find and risks data loss and creation of multiple copies of the same document which is poor practice. Save them under 'Files' in the Team.
- Download copies of files from Teams, this creates duplicate and potentially outdated copies.