Team Defence Information

IT Security Policy

Version	1.2
Author(s)	Will Tuohy & Tony Butler
Published date	19/05/2022
Review date	1/05/2024
Review date	30/07/2025

1. Background

Due to the nature of Team Defence Information's (TD-Info) business supporting the UK Defence Industry and Ministry of Defence, all employees are subject to a higher level of risk from malicious actors. This policy sets out the principles and overarching controls TD-Info operates to maintain minimum security standard. We do however encourage all staff to further strengthen their security where possible. Guidance for further security measures can be found here: https://www.ncsc.gov.uk/cyberaware/home

2. Scope

This information policy document applies to all permanent, part-time, temporary staff, consultants and volunteers using TD-Info or personally owned computing equipment on TD-Info business. It details the standards and procedures necessary to connect to TD-Info network equipment, servers, routers and storage media and provides guidance on safely writing, modifying or storing electronic documents or accessing material via internet or web technologies.

The majority of TD-Info's IT services are managed by our 3rd party IT solutions provider iTeam Solutions. The service agreement and full scope of the service can be found here (Service Agreement & iTeams Asset Register). The controls detailed below represent additional measures or activities which are the responsibility of TD-Info staff and contractors.

3. Information

3.1. UK Government and Ministry of Defence information

3.1.1. Team Defence Information operates as a not for profit trade association supporting the UK Defence landscape between industry and the Ministry of Defence. However, the highest level of classification that TD-Info will undertake to receive, transmit and store is UK Official.

3.1.2. In the event that information is received electronically that is above UK Official the information is to be fully deleted (deleted and removed from trash folders on the computer or email) and the incident reported to JSyCC WARP DefenceWARP@mod.gov.uk as per ISN 2017/03 (ISN 03/2017: Requirement to report security incidents affecting MOD material to the the MOD (publishing.service.gov.uk))

3.2. Storage

3.2.1. TD-Info maintains three platforms for the storage and dissemination of information:

3.2.2. Kahootz workspaces

3.2.2.1.1. Purpose: An online collaborative portal to enable TD-Info staff and select members to upload, store and update documents, images and videos that are pertinent to their working group, community or event.

3.2.2.1.2. Access & controls: All TD-Info staff and contractors have an account on the platform and utilise a dedicated 'TD-Info Task Team' workspace area. TD-Info members are added to dedicated workspace environments for events, working groups and communities on an as needed basis and licenses are provided to support this access. All users of the Kahootz platform provided by TD-Info have an individual account and set their own passwords.

3.2.3. UKCEB sharepoint

3.2.3.1.1. Purpose: Online storage for TD-Info task team for backups, meeting recordings

3.2.3.1.2. Access and controls: All TD-Info staff and contractors have access to this sharepoint site through their M365 package with rights to upload, download and edit documents in the enviroment only.

3.2.4. Teamdefence.info website

3.2.4.1.1. Purpose: Public dissemination of TD-Info events, activity outputs and governance.

3.2.4.1.2. Access and controls: All TD-Info staff have access to content creation, document upload and management of site users through logging in to a dedicated account using their TD-Info email and user set password.

3.2.4.1.3. TD-Info members are able to have an account created for them to access 'member only' areas of the site for events, content and documents that are intended for members only.

3.2.4.1.4. Non-TD-Info members and public are able to access and view the site without any log in but are only able to see pages and information that has specifically been published to the public. This is a manual control on documents and links uploaded to the website with three options – Private/ Staff Only: only TD-Info staff accounts are able to view and download the document; Members only: Only TD-Info member accounts and staff can view and download the document; Public: Anyone with access to the link can view and download the document.

3.3. Format of documents

3.3.1. The majority of Team Defence Information documents are in Microsoft Word, Powerpoint or Excel format.

3.3.2. TD-Info staff are to consider the appropriateness of the format for the document's audience. In principle, all documents that are to be shared publicly or with large groups of members the document should be saved in PDF format to discourage removing information from its context.

3.3.3. Where documents are in draft or being worked on by staff and members, the originator or custodian of the document should ensure it is only shared to relevant colleagues.

3.3.4. Email dissemination of the document should only be utilised after considering using a Kahootz workspace or Sharepoint site as these allow for greater control of access.

4. Assets

4.1. Network Equipment & Routers

4.1.1. This section is divided into assets which support the TD-Info office at Briarlands and those assets used by consultants when working from home

4.1.2. TD-Info office network equipment and routers

4.1.2.1. These assets are delivered and supported by iTeam which are detailed in the relevant section of the Asset Register and included in the service provision document

4.1.3. TD-Info BYOD assets

4.1.3.1. These assets are personal routers and connections used by TD-Info consultants and staff when working from home. These assets should have as a minimum WPA encryption and maintain a password that complies with the password principle of larger than 8 characters, complex and difficult to guess.

4.1.3.2. All other measures for BYOD are covered in the BYOD Policy (Link)

4.2. TD-Info computers

4.2.1. All Team Defence Information supplied assets for use by TD-Info staff (and consultants by exception) are managed by iTeams with admin rights locked to dedicated iTeams staff. All TD-Info assets come pre-loaded with Endpoint encryption and user accounts linked to the Office365 accounts which are authorised by the TD-Info Secretariat and managed by iTeams.

4.2.2. All iTeams supplied assets include ITAG reference numbers to identify them and are kept up to date and secure as per the service agreement with the provider.

4.3. Asset register

4.3.1. TD-Info maintains a single asset register in its Kahootz shared enviroment which is subject to an annual check.

4.3.2. This asset register includes a record of all BYOD along with iTeams supplied assets and is updated as TD-Info consultants and staff join or leave the organisation.

5. Account & Access Management

5.1. TD-Info users

5.1.1. Team Defence Information accounts are intended for staff and consultants. All qualifying colleagues receive a Microsoft 365 account with an associated @teamdefence.info email. This account enables access to the M365 suite of programs for use to conduct TD-Info business. Utilisation of this account to access services from a personal asset is allowed recognising the majority of TD-Info staff operate on a consultancy basis and do not receive dedicated TD-Info assets to conduct their work.

5.1.2. Normal TD-Info staff accounts do not allow access to console or admin permissions for the M365 domain or programmes. These permissions are held by our IT delivery partner iTeams. Account privileges can be elevated for individual staff for specific purposes and are removed once that purpose is fulfilled.

5.1.3. Provision of these accounts is the responsibility of the TD-Info Office Manager who requisitions an account through TD-Info's IT delivery partner, iTeam, as part of the onboarding of new staff.

5.1.4. In the event of a staff member leaving the organisation, iTeam will be notified and the account suspended within a timeframe negotiated with the departing colleague and the TD-Info Office Manager to enable the migration of any personal information or to ensure onward communications are established. This period will be no longer than 3 months.

5.1.5. Once the account is suspended, TD-Info will hold the account for no longer than 3 months before instructing iTeam to delete the account. This is to ensure any links and contact to that account can be forwarded to the relevant colleague.

5.1.6. Recipients of TD-Info M365 accounts must not share any passwords or allow anyone else to access and use the account.

5.1.7. The @teamdefence.info account will be the preferred account to assign access and account privileges for using the TD-Info website and Kahootz platform. These accounts will be provisioned by TD-Info staff with relevant permissions (managers/ super users) but will require colleagues to set their own passwords.

5.2. Privileged Account Management

5.2.1. Access to console and admin rights to the TD-Info Office 365 domain and applications is controlled by our IT delivery partner, iTeam.

5.2.2. Where admin rights are transferred to a TD-Info staff account, this must be for a specific business purpose and be requested in conjunction with the TD-Info Office Manager or Managing Director as appropriate.

5.2.3. Accounts with elevated privileges must enable 2-factor authentication in order to access elevated privilege services such as the Teams domain console.

5.2.4. Time spent operating with elevated rights must be minimised where possible and the user must not access their emails or download from websites (outside M365) whilst logged in with elevated privileges.

5.2.5. Users with elevated rights must not use mobile devices (phones or tablets) to access elevated rights areas of the TD-Info domain. Users must instead use laptops or desktops with compliant firewalls and antivirus software installed.

5.2.6. Such privileges should only be retained for as long as necessary. Where this is in support of a specific task, the rights should be downgraded on completion of the task. Where colleagues may have elevated privileges to support development or normal business management, these accounts should be reviewed by the Office Manager, Managing Director or Security Lead as appropriate on a frequent basis (no greater than 6 month intervals between reviews).

5.2.7. Operating under the principle of 'least privilege', there is no business reason for the transfer of full admin rights to a TD-Info staff member and such requests will be refused by Office Manager/ Managing Director. Requests must be made only for specific rights fitting a pertinent business need.

5.2.8. Should a staff member with elevated privileges leave TD-Info, it is the responsibility of the Office Manager to ensure that the elevated permissions are removed from their account immediately before referring to the account removal process for normal users stated in 5.1.4 - 5.1.6 of this policy.

5.3. TD-Info Members

5.3.1. All TD-Info member companies' staff can request accounts for the TD-Info website (www.teamdefence.info). These accounts can be requested through the website, requiring the user to register with their company email address. These requests are then reviewed by the Admin and/or Office Manager and approved as long as the request is from a recognised member company domain by cross checking the account request against the domain list for member companies.

5.3.2. In addition, member accounts can be created by TD-Info staff directly on the website by entering the requesting member's company email into the 'add user' console on the TD-Info website by TD-Info staff with admin permissions for the site. It is the responsibility of the TD-Info staff member creating the account to ensure that the email entered is from a recognised domain of a TD-Info member company. They are encouraged to consult with the TD-Info Office Manager, Managing Director or relevant Customer Relations Executive if they are unsure if the requested account belongs to a member company.

5.3.3. Special care and attention must be made to the domain extensions on requested accounts (e.g. @memberdomain**.[domainextension]**) as these are common indicators of spoofed or illegitimate accounts. TD-Info staff must refer to previous emails, contacts within a member company or the consult with the TD-Info Office Manager or Managing Director for confirmation of unrecognised domains.

5.3.4. TD-Info member accounts on the TD-Info website will have permissions to view and interact with content marked for 'members only' but do not have the ability to upload or create events as standard. These rights can be assigned to TD-Info member accounts on an exception basis where the contact is leading a task or activity where such rights

are appropriate. Such permissions will be bound to the completion of the task or activity that requires it and it is the responsibility of the assigning TD-Info staff member to assign and remove these rights in a timely fashion.

5.3.5. Where a member company ceases to be a member of Team Defence Information, accounts relating to that member company must be reviewed. It is the responsibility of the Managing Director of Team Defence Information to instruct the Office Manager and Administrative staff on the action to take. Depending on the circumstances of the company's departure, TD-Info staff may be instructed to suspend or remove accounts associated with that company. Exceptions for individuals may also be made but these accounts must then be converted into 'Guest' accounts to enable them to be monitored and tracked.

5.4. Guest Accounts

5.4.1. Guest accounts can be created for non-member individuals as an exception. These accounts can only be created by TD-Info staff members with the relevant permissions.

5.4.2. When creating a guest account, the TD-Info staff member must seek written authorisation from the Managing Director to create an account.

5.4.3. In principle, these accounts are for supporting prospective companies make the business case to become members, manage contributions from individuals who are embedded in TD-Info activities but may no longer belong to a member company or any other acceptable exception authorised by the Managing Director of TD-Info.

5.4.4. Guest accounts have the same level of access as full TD-Info members. However, these accounts are subject to review (intervals no greater than 6 months between reviews) and will be removed if the exception case no longer applies on challenge in review.

6. Electronic communications

6.1. Email

6.1.1. All TD-Info staff and consultants use the Office365 Outlook account for receiving and sending emails on TD-Info business.

6.1.2. iTeams have deployed a Quarantine filter on via Hornet Security which should sift the majority of incoming threats. Care should be taken by TD-Info staff and consultants when 'releasing' these emails by double checking the sender address and ensuring the email was expected. Any email labelled as a threat by this system cannot be released by the user and in the event of a legitimate email being mislabelled it is the responsibility of the TD-Info staff member to flag this to iTeams so they can investigate and either confirm the threat of calibrate the tool as appropriate.

6.1.3. Despite this tool, some unsolicited and malicious emails may still be delivered to TD-Info staff and consultants. As such the following basic principles should be always observed:

6.1.3.1. **Check the email is correct** – spoofed or malicious emails often appear to be from people you may know but with small typos in the name or domain. Always double check that the email matches what you were expecting before clicking any links or attachments.

6.1.3.2. **Distrust out of character requests and/ or urgency** – malicious actors often use urgency in email content to provoke a response. Always sense check requests and if doubt remains, call the individual before responding to or actioning an email. NEVER use the number in the suspect email, always use the numbers you or your colleagues have on file.

6.1.3.3. **If its too good to be true, it probably is** – whilst malicious and scam emails which offer reward or enticement are commonly recognised now, malicious actors often do find inventive ways to recreate old methods. As such all staff should operate on the principle that if its too good to be true, it probably is.

6.1.3.4. **Never click links, download attachments or forward emails which you suspect**. Always instead consult a colleague or the Managing Director and when in doubt, delete the email.

6.1.4. In the event of a legitimate email being sent to TD-Info by mistake (where an email may be Company Proprietary/ Sensitive or Official Sensitive and above) these emails must be fully deleted immediately by deleting from the users inbox and then further deleting them from the 'trash' folder in Outlook. For Official Sensitive and above instances the process detailed at 3.2.2 must also be followed.

6.2. Virtual Meetings & calls

6.2.1. All TD-Info staff and consultants have access to Office 365 Teams accounts on their @teamdefence.info domains. All TD-Info staff and colleagues are to use these accounts when conducting or joining virtual meetings on Teams.

6.2.2. Where a member company sets up a meeting on a different virtual platform (Zoom, Google Hangouts etc) TD-Info staff and consultants are to use their TD-Info emails to sign in or register to join such events

6.2.3. When in TD-Info facilitated or led virtual meetings, it is good practice to ask anyone that has 'dialled in' to the call via phone to identify themselves prior to commencing the meeting. In the event of someone dialling in whilst the meeting is underway, TD-Info staff and consultants should use natural pauses in the meeting (i.e. when moving on to another agenda item or discussion topic) to request dialled in attendees again identify themselves. This is a useful measure for capturing who is attending meetings but also serves as a mitigation against people who may be on the call without being invited.

6.2.4. TD-Info meetings cannot be held accountable for sharing of information to unintended individuals but the mitigation detailed in 6.2.3 does help to manage the situation.

6.2.5. Any and all recordings of TD-Info meetings must not be shared with a broader audience without the permission of those in the session (gained by asking for permission before turning on the recording function) and specific agreement of any colleagues that may have presented material.

7. Applications

7.1. All TD-Info staff members and consultants are to use Microsoft 365 (license and account will be supplied when onboarding) for the majority of their work.

7.2. Where other software or apps are required by a TD-Info staff member or consultant they are first to consult the approved application list held on the Business Management System and records in Kahootz.

7.3. If a TD-Info staff member or consultant requires the use of an app not included in the current list, they should consult with the company secretariat and/or Managing Director to discuss the requirement.

7.4. All applications must be acquired through a recognized vendor i.e. Microsoft Store, Google Play Store or Apple App Store.

8. Policy

8.1. It is the responsibility of TD-Info staff, contractors, and appointees from member businesses with remote access privileges to the TD-Info network to ensure that their remote access connection is given the same consideration as the user's on-site connection to their home companies.

8.2. General access to the Internet for recreational use by immediate household members through the TD-Info network on personal computers is permitted; however, the TD-Info staff member is responsible to ensure the family member does not violate any TD-Info policies and does not perform illegal activities.

9. Policy Compliance

9.1. Compliance to TD-Info policies is a requirement for working with Team Defence Information. Any noncompliance with policies will be subject to review and appropriate sanction by the Team Defence Information Managing Director.

9.2. Any staff found to have violated this policy may be subject to administrative action, which may include termination of engagement or, for non-compliances involving Government-owned data, further official disciplinary process.

10. Compliance Measurement

10.1. The TD-Info Secretariat - or other compliance body contracted by TD-Info MD - will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.

11. Exceptions

11.1. Any exception to the policy must be approved by the Company Secretariat or TD-Info MD in advance.

12. Related Standards, Policies and Processes

12.1. Bring Your Own Device Policy

12.2. Approved Application list

13. Revision History

Date of Change	Responsible	Summary of Change
6 Feb 2023	G NSMITH	V1.2 Changed TDI to correct TD-Info abbreviation