|  |  |
| --- | --- |
| Media Raid:2016 Branding Elements:1 - Logo:AI versions:New_DE&S_logo_RGB:Colour_RGB:New_DE&S_logo_RGB.png | Return form to::SOURCE:icons-for-form.jpgDESPSyA-SecurityAdviceCentre@mod.uk |
| ListXtranet Account Application |  |

* ListXtranet is the workspace used by the Defence Equipment & Support Principal Security Advisor (DE&S PSyA) to share government and defence security policy and guidance to HMG List X facilities. This workspace is hosted on the Defence Share collaborative working environment.
* Before submitting this application form you must consult the rules of use at Annex A.
* Submit this form as an email attachment to DESPSyA-SecurityAdviceCentre@mod.uk.

|  |  |
| --- | --- |
| **Forename(s)**      | **Surname**      |
| **Title**      | **Date of birth** *(for verification purposes)*      |
| **Email address***Provide the email address you wish to use for the account. This must be a professional email address registered through your organisation. This must not be a multi-user email address.*      |
| **Telephone number**      |
| **Organisation***Provide your organisation’s name.*      |
| **Position***Provide the security role you fulfil for your organisation e.g. Primary Security Controller.*      |
| **Location(s)***Provide details of all List X facilities for which you fulfil the above role. Please include postcodes.*      |
| **Other information***Are you replacing somebody else as the ListXtranet user for your location(s)? If yes, please provide details.*     *Please confirm all HMG departments for whom your organisation is a higher classification contractor (List X) e.g. MOD, ONR.*      |

Annex A to

ListXtranet Account Application

## ListXtranet Rules of Use

1. Only the registered primary Security Controller at a List X facility will be eligible to apply for a ListXtranet user account at this time. This will be reviewed on an ongoing basis.
2. You must read and agree to the Defence Share Security Operating Procedures (SyOPs) before creating your user account. These can be found:

under ‘Terms and Conditions’ when creating your account;

on your ‘Dashboard’, once logged in;

at Annex B of this document.

1. You should have a minimum of Security Check (SC) level clearance.
2. Defence Share is approved for the storage and processing of information broadly classified OFFICIAL. DE&S PSyA has been permitted to share OFFICIAL-SENSITIVE government and defence security policy on the platform by the respective Information Asset Owners (IAOs). You must obtain the informed approval of your respective IAO before sharing any OFFICIAL-SENSITIVE information on the platform.
3. You must not use the platform to share information with special handling requirements such as ITAR or IPR, or international classified information.
4. You must only access the platform using devices approved to store and process OFFICIAL-SENSITIVE information. The security requirements for processing OFFICIAL-SENSITIVE information can be found at Appendix 2 of the [Contractual Process document](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367491/Contractual_Process.pdf).
5. Government security policy published on the platform should not be supplied to anyone outside of your location’s security team or without a clear need-to-know. OFFICIAL-SENSITIVE information must not be disseminated over insecure networks or the internet at any time. If you need to share information beyond your security team, firstly consider updating your Company Security Instructions (guidance can be found in the [Security Requirements for List X Contractors document](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367514/Security_Requirements_for_List_X_Contractors.pdf)). Otherwise, you must seek guidance and approval from the Security Advice Centre.
6. **User Accounts.** You must ensure to adhere with the following requirements:
	1. When you are invited to join ListXtranet, you will receive an email from the Workspace Manager (or deputy). From this email they can access the Defence Share website and can create an account including setting a user name and password.
	2. All user account names must be based on an official and unique email address that can only be accessed by the user. Multi-user email accounts must not be used.
	3. You must not reallocate your Defence Share account to another individual, or otherwise share your password with and/or provide illegitimate access to another individual. If you no longer need to access ListXtranet, the Security Advice Centre should be notified so that the account can be removed. The process for inviting new users to a workspace should be followed if a new account needs to be created for an incoming member of staff.
7. **Passwords.** You must ensure to adhere with the following requirements:
	1. Passwords must be at least 9 digits long and must contain a combination of letters, numbers and special characters. They should not be based on common words, personal reference information (e.g. birthday, family names, etc) or have repeating characters (e.g. AAAAA111\*\*)
	2. Passwords will expire after 90 days after which the user will be prompted to select a new password. An old password cannot be re-used.
	3. If a user forgets their password there is an option to request that the password is reset and an email containing a new temporary password will be sent to the user’s email account. Once logged on, the user should immediately set a new password.
	4. If an incorrect password is entered 5 times in succession, the account will be locked and the user will need to request a password reset from the Workspace Manager.
8. **Security incidents.** In the event that an information security incident occurs, you must report this in accordance with [Industry Security Notice 2014/0](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/293480/ISN2014_02_Incident_Reporting.pdf)2.
9. **System support.** There are a number of support options for Defence Share, the most appropriate of which will depend on the specific need:
	1. In the first instance, perform checks to determine if the access or performance issue is caused by your company’s internal infrastructure. Incidents should be raised with your local service provider in accordance with local operating procedures.
	2. **Kahootz Support.** If the local service provider determines the cause lies with Defence Share, you should contact the Defence Share service provider for support. There are three methods by which support can be accessed. In order of preference, they are:
		1. **Kahootz Knowledge Base (KB).** The KB provides detailed information about all of the Kahootz functionality and so should be the first place to check. The KB is regularly updated and so can be relied on as an accurate source of information.
		2. **Raise an online support ticket.** Support tickets can be raised online using one of the support levels listed below. It is essential users read “Important Notice 2” below before submitting support tickets requests. This is the fastest method for requesting support from Kahootz
		3. **Email support.** If the online support is not accessible, then users can raise a support request by emailing support@kahootz.com. The following “Important Notice 2” also applies for emails but importantly, users should remove their organisation/location details from their signature blocks before sending the email because these will appear in the support call.

The Kahootz Support Desk records all support requests onto DeskPro, an Amazon Web call logging service hosted in the US. This applies to support requests raised via the Kahootz online ticketing service or submitted by email. DeskPro will store information such as user names, user email addresses, workspace names, site name (i.e. Defence Share) and details of the support request. You must ensure that support requests do not contain any sensitive or inappropriate information. For example, refrain from providing your organisation and location details. Furthermore, it is not appropriate to disclose user password details to the Kahootz Support Desk under any circumstances, either by telephone or online support. Adherence to these rules is a critical pre-requisite for accreditation and so support requests will be audited to ensure conformance.

Annex B to

ListXtranet Account Application

## Security Operating Procedures (SyOPs) for Users of the Defence Share Collaborative Working Environment

Version 1, 9 Oct 2015, OFFICIAL

## Introduction

1. This document constitutes the Security Operating Procedures (SyOPs) for Defence Share. All references to Defence Share refer to the capability hosted within the Kahootz application procured through the Digital Marketplace and provided by Inovem. They are issued by the Defence Share Project Manager in accordance with the above references and have been approved by the MOD DAIS Accreditor.
2. All personnel, both MOD and from external organisations, who access Defence Share are to comply with these SyOPs. References A-D apply to all users. For Acceptable Use and Security Incident reporting users must follow the document commensurate to their employing organisation. No departure from, or amendment to them, is permitted, unless prior authorisation is obtained from the DAIS Accreditor. By signing Annex A to this document users are agreeing to comply with these instructions. Customer Workspace Owners MUST retain a copy of the user agreement for future compliance audits.
3. A copy of this document is to be retained by all users.
4. Non compliance with these SyOPs is likely to render the offender liable to removal of access to Defence Share. Access will only be re considered on the agreement of the Defence Share Accreditor (who reserves the right to refuse re-enabling the account).
5. Direct access to Defence Share is the responsibility of the Individual Business Units. Access is controlled by the Workspace Manager and is limited to those personnel listed by the Workspace Manager as having signed Annex A. This includes confirmation that the SyOPs have been read and understood before using Defence Share.
6. A Defence Share Workspace Manager will provide all authorised users of the service with a username and password as per the procedure provided in the Defence Share User Guide. A list of approved users will be maintained by each Defence Share Workspace Manager.
7. The SyOPs informs all personnel accessing Defence Share what they can and cannot do. The SyOPs are designed to assist in the efficient operation of this environment. Failure to follow the procedures could lead to a breach of Confidentiality (the restriction of information to those authorised to receive it), Integrity (the assurance that information has been created, amended or deleted only by the proper actions of authorised users) or Availability (timely access to assets by authorised users).
8. The Defence Share User Guide provides intuitive information to support its use and this is supplemented by the SyOPs which must be understood and adhered to. Regular internal and external audits will be conducted to ensure that the procedures are being followed – these will be part of the re-accreditation process and will be managed by the ISS Defence Share Security Assurance Manager.
9. The Defence Share User Guidelines v1.2 dated 8 October 2015 must be read in conjunction with these SyOPs.

## Protective Marking

1. Defence Share is approved for the storage and processing of**up to OFFICIAL**, where this includes information deemed to be **OFFICIAL SENSITIVE** users must be prepared to accept the additional risks which this attracts and consider carefully whether Defence Share is appropriate. As described in the Defence Share User Guide this should preferably be on an exceptional basis. The Government Security Classification (GSC) Guidance should be consulted.

## External ISS Defence Share Users

1. All external users of Defence Share, gaining access from their own organisation must comply with these SyOPs ensuring their own employees are appropriately trained and aware of Information Security procedures within their own organisation.
2. External Users will have to confirm through compliance with a Security Aspects Letter (SAL) that their premises will be suitable for the storage of OFFICIAL data and that they have personnel vetted to the minimum of Baseline Personnel Security Standard (BPSS), or equivalent, for viewing OFFICIAL data. Defence Share Workspace Managers shall not provide access to external users without the prior approval of the relevant Project Team and/or Commercial Team. Where OFFICIAL SENSITIVE data is to be shared, even on an exceptional basis, the SAL must state this applicability.
3. A list of authorised users will be retained and managed by the Defence Share Workspace Manager. The ISS Sys Admin will have access to the master system logs that may be used to support forensic activities with respect to security incidents. Any change to the list of authorised users must be approved by the Defence Share Workspace Manager. Any anomalies are to be notified to the ISS Defence Share Sys Admin.
4. Only authorised Defence and Industry email accounts are to be used for Defence Share business. For example, there should be no use of hotmail, gmail etc email.

## General Procedures for All Defence Share Users

All Defence Share users shall adhere to the following instructions.

1. Read training material provided to ensure appropriate use of Defence Share. Where required attend and implement any appropriate training.
2. Report all security incidents involving a breach of personnel, software, communication, document or physical security immediately in accordance with Reference F. Defence Share users from external organisations should inform their Company Security Controller and Workspace Manager. The Workspace Manager must then follow "2015DIN02-004 - MOD Security Incident Reporting Process"
3. Loss of hardware should be reported as identified at paragraph 16.
4. Log off computers and laptops (unless a password protected screen saver is in operation on the workstation) when unattended. When you have finished a session on the workstation invoke the password-protected screensaver and at the end of work close down and log off the application.
5. If, in an emergency, you need to leave the office quickly, e.g. a fire alarm, invoke the password-protected screensaver, ONLY IF IT IS SAFE TO DO SO, so that unauthorised personnel cannot use it.
6. Remember that it is a fundamental principle that knowledge or possession of Protectively Marked information must be strictly limited to those staff that have a need to know. Users working on documents in Defence Share must adhere to this principle.
7. Comply with all References as stated above and any local security procedures. MOD users must comply with all references as stated above. For external users references A-D apply and additionally their own organisational Acceptable Use Policy and Security Incident reporting process apply. Local security procedures must be followed.
8. Notify the Defence Share Workspace Manager if your access requirements change. Access requirements for Defence Share will be allocated based upon your role.
9. Defence Share users shall not disable the anti-virus software resident on workstations or laptops.
10. Information protectively marked OFFICIAL SENSITIVE, even when residing in Defence Share for a short term, shall not be emailed to anyone without prior approval of the Information Asset Owner (IAO). This specifically refers to email over the Internet and/ or Insecure email networks.
11. Defence Share Workspace Managers/ users must ensure that they have the correct security clearance required to view the information contained within Defence Share. If they are in any doubt about their security clearance, they must contact their Security Controller for clarification before using the service.
12. Defence Share users must not permit shoulder surfing by any unauthorised user.
13. Defence Share users must not attempt to circumvent the controls that have been put in place to assist in supporting Defence Share.
14. Defence Share users must not attempt to gain unauthorised access to other controlled areas within Defence Share This includes attempts to access information outside of your normal access rights or duties. You will be responsible for all actions undertaken in Defence Share using your UserID.
15. The use of personal USB storage devices is strictly prohibited on a workstation which is connected to Defence Share. Local security policy and procedures should be consulted.
16. The Accidental loss, overlooking or eavesdropping are the greatest risks when an individual is required to work remotely on protectively marked information. Any laptop/ device used in a public place must be used with caution.
17. Where authorised USBs or other removable media, are in use e.g. CDs and DVDs these must be protected and handled in a manner commensurate with the highest protective marking of material processed on a workstation or device and the latest security instructions issued by the MOD.
18. Unless declassified by approved data destruction the protectively marked items of removable media must be retained and controlled appropriately until final approved disposal takes place.
19. Document and equipment disposal must conform to the regulations for the protective marking of OFFICIAL SENSITIVE as specified in HMG Information Assurance Standard Number 5 and JSP 440, Part 8.
20. Comply with the Defence Share rules on setting passwords, as stated in the paragraphs below.
21. You will be issued with a unique user ID and initial password to logon to application. You MUST change this password to one of your own choosing as soon as you log on for the first time. Passwords should use alpha-numeric characters and be non-dictionary.
22. Do not base your password on common dictionary or slang words, or on repeating characters (i.e., AAA111\*\*). Passwords are not to be recycled. The password history limit is set to 12.
23. Your password must consist of a minimum of 9 alpha-numeric characters. This password will be changed at least every 90 days.
24. Attempts to use the application under another identity (UserID) or share your password with anyone else are strictly prohibited.
25. Defence Share users must not disclose their password to anybody. Should it be suspected, or known, that the password has been compromised, the password must be changed immediately and, where appropriate, this suspicion reported to the Defence Share Workspace Manager, the Local Security Officer, MOD or Industry Security Controller in accordance with Reference F.

## Workspace Manager Procedures

1. In addition to the general procedures for all users the workspace managers must not abuse their privileges. The Workspace Manager responsibilities detailed in the Defence Share User Guide (ref H) must be adhered to.
2. Workspace Managers must only create authorised workspaces. When the need for a workspace ceases then removal procedures should be followed, off-boarding procedures as covered in the Defence Share User Guide should be followed.
3. Care must be taken when inviting new people to the workspaces from the perspective of need to know access, licence consumption and cost implications. Workspace Managers must ensure that all Users who are added to a workspace have the correct clearance for that workspace.
4. Workspace Managers must undertake regular housekeeping activities to ensure authorised access to their workspace remains current.
5. In addition to the general procedures for all users the workspace managers must not abuse their privileges.

## Site Administrators Procedures

1. Site Administrators must not undertake administrative actions without the appropriate audit trail of the request.
2. Site Administrators will access the Admin app with 2 Factor Authentication.