BDAU SE Policy Documents

This directory contains all BDAU SE policy documentation as per below:

- BDAU SE Access Control Policy
- BDAU SE Asset Management Policy
- BDAU SE Business Continuity Policy
- BDAU SE Change Management Policy
- BDAU SE Corrective And Preventative Action Policy
- BDAU SE ISMS Manual

BDAU SE Access Control Policy

Document Number	75442441
DR Document Number	75440184
Content Approval	See comments for version / approver
Version Number	24
Previous Active Version Number	23
Review Cycle (months)	12
Document Type	Policy
Last Modified Date	Aug 31, 2021 13:24

This document is the Access Control Policy. It describes the Big Data and Analytical Unit (BDAU) policy for access control within the BDAU Secure Environment (SE).

Scope

This policy covers information assets held or equipment operational within the BDAU SE. For a list of qualifying assets see the BDAU SE Asset Registry SOP. The scope of this policy covers access for the following:

- Provision of access to the BDAU SE
- Provision of access to information assets within the BDAU SE

For a list of legal and regulatory requirements which we operate by see the BDAU SE ISMS Manual.

Responsibilities

Within the scope of this document the following responsibilities apply:

1. Information Security Manager (ISM) - The ISM has overall responsibility for information governance and security within the BDAU SE. The post holder is responsible for the management of Information Security Policy (ISP) as per the BDAU SE ISMS Manual and ensuring the appropriate mechanisms are in place to support service delivery and continuity.
2. Information Asset Owner (IAO) - The IAO has overall responsibility for data contracts and data management relating to one or more information assets held within the BDAU SE as indicated by the BDAU Asset Registry and maintained according to the BDAU SE Asset Registry SOP. The IAO is responsible for approving access requests for owned information assets, ensuring the use of an information asset abides by the data processing agreement or data controller requirements for their assets and for ensuring that users of an asset notify the BDAU immediately of any actual or suspected breaches as per the BDAU SE User Registration Form.
3. Information Asset Administrator (IAA) - The IAA is the day to day contact for an information asset and can coordinate activities including access approvals and asset modification requests on behalf of the IAO with IAO permission. This does not delegate the responsibilities of the IAO however and ultimately the IAO will be held accountable for any misuse of information assets as a result of asset users or administrators. The BDAU will act as the default asset administrator for all information assets if not otherwise named. The IAA can be a non-employee of the College so long as they have the permission of the IAO to be IAA.
4. BDAU SE Staff - The staff of the BDAU in regards to the BDAU SE will abide by ISP as per the BDAU SE ISMS Manual.
5. BDAU SE Users - Users of the BDAU SE or information assets held within the BDAU SE will abide by the ISP as per the BDAU SE ISMS Manual.

User Access Management

User Registration

The life-cycle of user access in the BDAU SE, from the initial registration process of new users to the final de-registration of users who no longer require access, is controlled through a formal user registration procedure as per the BDAU SE User Registration SOP. All users with access to the BDAU SE infrastructure must have a valid (non-expired) user registration form. Access granted by user registration does not control access to datasets within the BDAU SE, this is controlled through the BDAU SE Dataset Registration SOP.

De-registration of Users - Revoking Access

Users who do not renew their user registration as per the BDAU SE User Renewal SOP will lose access automatically to the BDAU SE infrastructure, including all information assets (datasets) held within the BDAU SE. This is done automatically on the BDAU SE platform, regardless of status in the access distribution list.

Dataset Access Management

Dataset Registration

User registration only grants access to login to the BDAU SE, it does not grant access to dataset information assets held within the BDAU SE. Access to dataset information assets within the BDAU SE is controlled by the BDAU SE Dataset Registration SOP. Users who require access to dataset information assets will require a valid (non-expired) dataset registration form.

De-registration of Users for Datasets - Revoking Access

If a user does not renew their dataset registration as per the BDAU SE User Renewal SOP, will lose access automatically to the relevant dataset information asset. Note that users without a valid user registration will lose access to all dataset information assets. Both of these items are done automatically on the BDAU SE platform, regardless of status in the relevant access distribution list.

Datasets Granted Under Exception

Where the BDAU cannot integrate dataset information assets into the BDAU SE, for instance where software requirements cannot be met, the BDAU will grant exception access to dataset information assets. Dataset information assets granted under exception do not fall within scope of BDAU SE ISO 27001 specifications and are not subject to the same requirements. This is covered by the BDAU SE Dataset Exception SOP.

Access Review

User and dataset access rights which are expired will be automatically removed as described above. In addition the BDAU will hold periodic access review audits to ensure that users hold only the access they require. This will involve spot-checking for random users with line managers to ensure the users still requires access and spot-checking for random dataset information assets with information asset owners to ensure the users all still require access. The outcome of these reviews will be managed according to the BDAU SE Corrective And Preventative Action Policy.

Privilege Management

"Special privileges" are those allowed only to BDAU SE staff as facility, systems and information asset administrators. This access may or may not include access to some or all data. The unnecessary allocation and use of special privileges is a major contributing factor to system vulnerability. Therefore special privileged access is to be strictly controlled and recorded and only permitted for BDAU SE staff. Access to privileged commands is controlled through the "sudo" authorisation system for unix and local admin privileges for windows.

Password Management

Login to the BDAU SE is strictly controlled. Multi-layered, Multi-Factor Authentication is required for all access. This is jointly managed by both College ICT and BDAU IT staff.

Where a user has forgotten their College Single Sign On password for the BDAU SE they need to contact College ICT to reset that. Where a user needs a new TOTP sequence (eg loss/change of Personal Electronic Device) BDAU staff are authorised to reset the user's TOTP sequence.

Remote Access

All access to the BDAU SE is controlled via the Imperial College Secure Gateway which wraps relevant sessions in a SSL encrypted layer. This includes BDAU staff working on-site or off-site. All access for BDAU staff and users is remote access and follow the same procedure for access. More information on the BDAU SE access procedure is available as per individual OS specific access guides under the BDAU SE Server Access SOP.

Building and Facilities Access

BDAU SE Staff Working Areas

BDAU staff working areas are protected by pin-coded locked doors with badge readers for external doors. BDAU SE staff and BDAU SE users are not permitted to share pin-codes for doors or to lend their badge to other individuals for access. A member of BDAU SE staff must be present at all times in primary BDAU SE working sites if other staff require access.

BDAU SE Server Facilities

Facilities where BDAU SE server equipment is held are accessible only by service personnel required for server maintenance as per the BDAU SE ICT MoU. Areas for storage and transfer of equipment for server purposes are protected as per the BDAU SE ICT MoU.

Monitoring and Audit

User and dataset information asset access will be subject to monitoring and review and the ISM will be responsible for working with both internal and external auditors to ensure that audits of the BDAU SE are conducted on a regular basis. The ISM will be responsible for ensuring that any breaches or risks that are identified are added to the BDAU SE Risk Registry as per the BDAU SE Risk Registry SOP.

Training

All users are required to complete training on an annual basis. This changes depending on what is available, see the BDAU SE User Registration SOP for the most recent training requirements.

Version	Change
20	Modified: On-site Access Section to reflect All on-site access is now per remote access.
21	Modified: On-site Access Section (removed "direct" from "BDAU staff working on-site in certain locations have direct access to the BDAU SE from their workstations")
22	Removed "Provision of access to workstations operated by the BDAU with direct access to the BDAU SE" from Scope as it is redundant (it is part of access) Removed "As of Q4, 2019 all IAOs must be substantial employees of the College, and will be required to sign asset owner agreements." as it has not been enforced yet. Typo fix in Dataset Registration section (de-registration to re-registration) Updated the link under Password Management section to link to the SOP rather than the draft
23	Updated User and Dataset Registration and De-registration (no allotted time for renewal, users lose access once their form expires) Removed "On-site Access" and updated "Remote Access" as all access (inlcuding BDAU staff working os-site) is remote access
24	ML-MFA detail added.

BDAU SE Asset Management Policy

Document Number	75442486
DR Document Number	75440809
Content Approval	See comments for version / approver
Version Number	28
Previous Active Version Number	27
Review Cycle (months)	12
Document Type	Policy
Last Modified Date	Sep 01, 2021 14:40

This document is the Asset Management Policy. It describes the Big Data and Analytical Unit (BDAU) policy for asset management within the BDAU Secure Environment (SE).

Scope

This policy covers information assets held or equipment operational within the BDAU SE. For a list of qualifying assets see the BDAU SE Asset Registry SOP. The scope of this policy covers access for the following:

- Information assets and information systems:
  - Databases
  - Datasets
  - Hardcopy documents
  - User guides
  - Notebooks
  - Training material
  - Policies, procedures
  - Business continuity plans
  - Financial data
- Software:
  - Applications
  - System software
  - Development software
  - Utilities
- Physical:
  - Computer equipment (servers and workstations)
  - BDAU staff areas
- Personnel:
  - Knowledge
  - Skills
  - Experience
- Intangibles:
  - Reputation

Responsibilities

Within the scope of this document the following responsibilities apply:

1. Information Security Manager (ISM) - The ISM has overall responsibility for information governance and security within the BDAU SE. The post holder is responsible for the management of Information Security Policy (ISP) as per the BDAU SE ISMS Manual and ensuring the appropriate mechanisms are in place to support service delivery and continuity.
2. Information Asset Owner (IAO) - The IAO has overall responsibility for data contracts and data management relating to one or more information assets held within the BDAU SE as indicated by the BDAU Asset Registry and maintained according to the BDAU SE Asset Registry SOP. The IAO is responsible for approving access requests for owned information assets, ensuring the use of an information asset abides by the data processing agreement or data controller requirements for their assets and for ensuring that users of an asset notify the BDAU immediately of any actual or suspected breaches as per the BDAU SE User Registration Form.
3. Information Asset Administrator (IAA) - The IAA is the day to day contact for an information asset and can coordinate activities including access approvals and asset modification requests on behalf of the IAO with IAO permission. This does not delegate the responsibilities of the IAO

however and ultimately the IAO will be held accountable for any misuse of information assets as a result of asset users or administrators. The BDAU will act as the default asset administrator for all information assets if not otherwise named. The IAA can be a non-employee of the College so long as they have the permission of the IAO to be IAA.

4. BDAU SE Staff - The staff of the BDAU in regards to the BDAU SE will abide by ISP as per the BDAU SE ISMS Manual. Furthermore the BDAU SE staff are responsible that assets are correctly labelled and can be audited with the appropriate registration and evaluation forms. The BDAU SE staff must also ensure that all assets that are required to be recorded are recorded in the BDAU SE Asset Registry SOP.
5. BDAU SE Users - Users of the BDAU SE or information assets held within the BDAU SE will abide by the ISP as per the BDAU SE ISMS Manual. Users are responsible to ensure that they understand and abide by the labels which are assigned to the assets they use as per the BDAU SE Information Classification SOP and to notify BDAU SE staff if any changes are required for those assets in terms of information governance, access or labelling.
6. Equipment and Facilities Managers - IT equipment including telecommunications devices, loading bays, physical assets, fire alarms and all site facility management is performed under MoU. For more information see BDAU SE ICT MoU.

Information Asset Handling

Security while handling information assets is of the utmost importance to the BDAU, its staff, its users and its partners. Mishandling of information assets whether intentional or unintentional will result in possible disciplinary action (for more information see the BDAU SE HR MoU) and loss of access to assets. All information assets supplied within the BDAU SE are not allowed to leave the BDAU SE unless an exception is granted, at which point those assets that have left the BDAU SE no longer fall into scope of these policies. All assets including assets granted under exception are recorded in the BDAU SE Asset Registry SOP along with the IAO and the asset users distribution list. Specific requirements for asset types include:

1. Dataset Assets - Dataset assets include any data for which the BDAU SE staff are responsible under ISO 27001 specifications. Access to dataset assets are granted within the BDAU SE using the BDAU SE Dataset Registration SOP and must abide by the access control policy described in the BDAU SE Access Control Policy. All dataset assets must be recorded in the BDAU SE Asset Registry SOP. Asset users for datasets can be contacted using the associated contact distribution list as recorded in the BDAU SE Asset Registry SOP. Furthermore all dataset assets should be transferred using secure channels as per the BDAU SE Dataset Evaluation SOP.
    a. Assets Granted Under Exception - Dataset assets which can not be held in the BDAU SE due to requirements which fall outside the services provided will require a BDAU SE Dataset Exception as per the BDAU SE Exception Registration SOP. These assets will still be recorded in the BDAU SE Asset Registry SOP so they can be investigated as a risk which requires remediation, but these assets will not fall under BDAU SE ISO 27001 specifications.
2. Vendor Assets - Vendor assets are metadata assets which are held by the BDAU to ensure ongoing ability to contact providers of data and software where required. This ensures compliance with regulation and vendor specific training. Vendor assets are created using the Vendor Evaluation procedure outlined in the BDAU SE Vendor Evaluation SOP. Vendor assets are recorded in the BDAU SE Asset Registry SOP.
3. External Services - External services which are required for the BDAU SE to maintain services according to ISO 27001 specifications are kept under BDAU SE MoU Documents.
4. Software Assets - Software assets include software used by or created by the BDAU as used within the BDAU SE. This includes:
    a. Applications - Software used within the BDAU SE and on BDAU SE staff workstations falls within scope of the BDAU SE ISMS Manual. All applications must be appropriately sourced using BDAU SE approved suppliers and must be evaluated according to the review of the ISM and must have a valid license for its intended users. All software used within the BDAU SE must be recorded in the BDAU SE Asset Registry SOP. Users must only have access to software for which they are licensed.
    b. System software - Server/system software such as operating systems must be evaluated to ensure they meet the same criteria as other applications as per above.
    c. Software Support - Software is kept within two major releases of the latest vendor/provider supported version at all times. Vendor operating system release selection ensures ongoing long-term support for at least the warranty lifetime of the hardware.
    d. Patch management - College ICT infrastructure is patched as per College ICT path management procedures. BDAU SE server infrastructure is patched regularly; the standard cycle is fortnightly. Pending patches are reviewed as they are published and applied immediately, if practical or if criticality demands. Otherwise they are applied within two weeks. Additionally, live patches and/or interim fixes may be implemented until such time as vendor patches can be installed.
5. Physical Assets - Physical assets include staff and user equipment in the BDAU SE. This includes but is not limited to:

    a. IT equipment - BDAU SE equipment includes servers which make up the BDAU SE and BDAU SE staff workstations. BDAU SE equipment is maintained in the BDAU SE Asset Registry SOP. Changes to the BDAU SE equipment such as hardware and software maintenance must be done according to the BDAU SE Change Management SOP and must abide by the change management policy as described in the BDAU SE Change Management Policy.
    b. Portable media storage - Information assets provided on portable media storage will be provided only under BDAU SE exception as per the BDAU SE Exception Registration SOP. Use of portable media devices is generally discouraged by the BDAU except where absolutely necessary. Where necessary portable media devices, including laptops, should be encrypted, password protected and if possible pin-protected.
    c. Backup tapes - Removable media for backups is controlled by an external service provider as per the BDAU SE ICT MoU. This includes secure transfer of tapes to archive.
    d. Local media storage - The BDAU recommends that all information assets are stored and used only on local media within the BDAU SE. The BDAU will make every effort to accommodate requirements in order to ensure this is possible. Where this is not possible exceptions will be granted according to the BDAU SE Exception Registration SOP. Policy for access to information assets stored on local media is covered by the BDAU SE Access Control Policy. Destruction of local media and information assets is done according to the BDAU SE ICT MoU.
    e. Physical paper records - The BDAU maintains a list of physical paper records which are also stored in electronic format (scanned). These include all registration and evaluation forms, signed MoUs, data vendor contracts and other miscellaneous records. Paper records which are not marked as risk score low (public and publishable) must be disposed of by placing the paper records in the confidential waste blue bins. All electronic records which are scanned are stored for a minimum of 10 years.
    f. Data storage - All data at rest is stored on disk in individual (per BDAU dataset), independent AES256-GMC encrypted filesystems. Upon data destruction, encryption keys for those filesystems are destroyed with a 38 pass, mixed mode (null/random/special/random) file deletion tool. Tape backup (network transfer and storage), provided and managed by College ICT, is secured with AES256 encryption. All data transfers initiated by BDAU staff are routinely secured with at least AES256 encryption. Data integrity is ensured at the hardware level (redundant disks), and at the kernel filesystem level through layout design (RAID-Z2, analogous to traditional RAID6) and via regular, monthly, checksum verification checks of all on-disk data. All data are secured within a AES256-GMC encrypted filesystem with access controls applied with per-user granularity inside per-project BDAU datasets, implemented via standard, traditional UNIX POSIX file permissions and UNIX POSIX.1e ACLs.

    g. Firewall - Outer, public-facing, primary firewall policy is managed by College ICT. Access is only granted to registered users. Inner, secondary firewall policy is managed by BDAU IT staff. Both firewalls default to deny.
    h. Network operation policy - to comply with relevant parts of Information Security, User Authentication and Access, Firewall, Software Support, and Patch Management policies.
6. Disposal of Assets - All BDAU SE assets must be disposed of securely whether physical or digital assets. Asset disposal procedures are covered by the BDAU SE ICT MoU. All data on disk are destroyed by secure deletion (38 pass, mixed mode) of the associated AES256-GMC encryption key. All hardware disks and backup tapes, at end-of-life/service, are destroyed by College ICT as per the BDAU SE ICT MoU. Where user personal electronic devices are replaced, lost, at risk or potentially compromised, BDAU SE TOTP token seeds (and thus TOTP sequences) are regenerated (replaced) thus rendering the previous user seed/sequence redundant and useless.
7. Locking of Screens and Clear Desks - All BDAU SE staff are expected to lock their screens when not at their workstations and to keep their desks clear of any sensitive information. BDAU SE staff working area procedures are covered in the BDAU SE Staff Working Areas SOP.

No BDAU SE assets are allowed to leave the BDAU SE without explicit permission of the BDAU SE ISM.

Information Asset Labelling

All information assets must be labelled as per BDAU SE Information Classification SOP.

Communication

All communication which is sensitive in nature will be conducted over secure channels whenever possible. This includes transfer of user credentials and passwords (as per the BDAU SE User Addition SOP), transfer of data into or out of the BDAU SE (as recorded in the BDAU SE Dataset Evaluation SOP), access to the BDAU SE (as per the BDAU SE Server Access SOP) and any other communication which requires encryption and security.

Version	Change
24	Typo fix in IAO name (manager to owner) and IAA (owner to administrator)
25	Reviewed: no major changes
26	Removed "As of Q4, 2019 all IAOs must be substantial employees of the College, and will be required to sign asset owner agreements." as it has not been enforced yet.
27	Amended: Communication with a link to the BDAU SE User Addition SOP
28	Added Network Operation, Information Security, User Authentication and Access, Firewall, Software Support, Patch Management, Data Storage, and Data and IT Equipment Disposal policies.

BDAU SE Business Continuity Policy

Document Number	75444900
DR Document Number	75444817
Content Approval	See comments for version / approver
Version Number	11
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	Policy
Last Modified Date	Feb 28, 2020 11:07

This document is the Business Continuity Policy. It describes the Big Data and Analytical Unit (BDAU) policy for continued and sustainable service delivery within the BDAU Secure Environment (SE).

Scope

This policy covers information assets held or equipment operational within the BDAU SE. For a list of qualifying assets see the BDAU SE Asset Registry SOP.

Responsibilities

Within the scope of this document the following responsibilities apply:

1. Information Security Manager (ISM) - The ISM has overall responsibility for information governance and security within the BDAU SE. The post holder is responsible for the management of Information Security Policy (ISP) as per the BDAU SE ISMS Manual and ensuring the appropriate mechanisms are in place to support service delivery and continuity.
2. Information Asset Owner (IAO) - The IAO has overall responsibility for data contracts and data management relating to one or more information assets held within the BDAU SE as indicated by the BDAU Asset Registry and maintained according to the BDAU SE Asset Registry SOP. The IAO is responsible for approving access requests for owned information assets, ensuring the use of an information asset abides by the data processing agreement or data controller requirements for their assets and for ensuring that users of an asset notify the BDAU immediately of any actual or suspected breaches as per the BDAU SE User Registration Form.
3. Information Asset Administrator (IAA) - The IAA is the day to day contact for an information asset and can coordinate activities including access approvals and asset modification requests on behalf of the IAO with IAO permission. This does not delegate the responsibilities of the IAO however and ultimately the IAO will be held accountable for any misuse of information assets as a result of asset users or administrators. The BDAU will act as the default asset administrator for all information assets if not otherwise named. The IAA can be a non-employee of the College so long as they have the permission of the IAO to be IAA..
4. BDAU SE Staff - The staff of the BDAU in regards to the BDAU SE will abide by ISP as per the BDAU SE ISMS Manual. Staff are responsible for supporting continued service.
5. BDAU SE Users - Users of the BDAU SE or information assets held within the BDAU SE will abide by the ISP as per the BDAU SE ISMS Manual.

Backup of Information Assets

Information assets, especially dataset assets, require backup plans for assets deployed in production. This allows assets to be restored in event of a disaster, unplanned outage or unexpected loss of access to information assets. Data assets for the BDAU SE are backed up as per the BDAU SE Backup SOP.

Restoration of Information Assets

Information assets can be restored both from local sources, such as in the event of accidental file deletion, or from tape archive, such as in the case of service restoration to a disaster recovery site. For more information on restoring information assets see the BDAU SE Backup SOP.

Information Classification

All BDAU SE information assets should have a classification for business continuity. This allows the BDAU SE to easily identify what would need to be restored during a disaster recovery situation or prioritise an asset for restoration during accidental deletion. For more information see the BDAU SE Information Classification SOP.

Business Continuity Management Testing

To ensure that critical systems and information assets which are deemed business critical can be available in the event of a disaster, unplanned outage or unexpected loss of access, business continuity management plans must be tested. These simulations provide confirmation that critical systems and information assets continue to be available as required. The business continuity classification as defined by the BDAU SE Information Classification SOP is recorded as per the BDAU SE Asset Registry SOP.

Staff Relocation

Staff will be relocated to a new site if the usual BDAU SE staff area is not available. Instructions for how to relocate will be available to BDAU SE staff in the BDAU SE Staff Working Areas SOP.

Version	Change
7	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
8	Amend policy to remove need for local backup which is not currently performed as per audit of Mar 2018
9	Updated IAO & IAA definitions according to asset management and access control policies
10	Reviewed: no major changes
11	Removed "As of Q4, 2019 all IAOs must be substantial employees of the College, and will be required to sign asset owner agreements." as it has not been enforced yet.

BDAU SE Change Management Policy

Document Number	75444889
DR Document Number	75444835
Content Approval	See comments for version / approver
Version Number	8
Previous Active Version Number	7
Review Cycle (months)	12
Document Type	Policy
Last Modified Date	Feb 28, 2020 11:25

This document is the Change Management Policy. It describes the Big Data and Analytical Unit (BDAU) policy for change management, delivery of upgrades and disposal of unnecessary assets within the BDAU Secure Environment (SE).

Scope

This policy covers information assets held or equipment operational within the BDAU SE. For a list of qualifying assets see the BDAU SE Asset Registry SOP.

Responsibilities

Within the scope of this document the following responsibilities apply:

1. Information Security Manager (ISM) - The ISM has overall responsibility for information governance and security within the BDAU SE. The post holder is responsible for the management of Information Security Policy (ISP) as per the BDAU SE ISMS Manual. This includes the provision of changes to the BDAU Secure Environment, procurement and introduction of new assets and archiving or disposal of assets no longer required.
2. Information Asset Owner (IAO) - The IAO has overall responsibility for data contracts and data management relating to one or more information assets held within the BDAU SE as indicated by the BDAU Asset Registry and maintained according to the BDAU SE Asset Registry SOP. The IAO is responsible for approving access requests for owned information assets, ensuring the use of an information asset abides by the data processing agreement or data controller requirements for their assets and for ensuring that users of an asset notify the BDAU immediately of any actual or suspected breaches as per the BDAU SE User Registration Form.
3. Information Asset Administrator (IAA) - The IAA is the day to day contact for an information asset and can coordinate activities including access approvals and asset modification requests on behalf of the IAO with IAO permission. This does not delegate the responsibilities of the IAO however and ultimately the IAO will be held accountable for any misuse of information assets as a result of asset users or administrators. The BDAU will act as the default asset administrator for all information assets if not otherwise named. The IAA can be a non-employee of the College so long as they have the permission of the IAO to be IAA.
4. BDAU SE Staff - The staff of the BDAU in regards to the BDAU SE will abide by ISP as per the BDAU SE ISMS Manual. Staff are responsible for supporting continued service. BDAU SE staff are responsible for ensuring no changes are made outside of change management policy.
5. BDAU SE Users - Users of the BDAU SE or information assets held within the BDAU SE will abide by the ISP as per the BDAU SE ISMS Manual. BDAU SE users are expected to abide by plans of change management as informed and not interrupt indirectly or directly with changes as they occur.

Change Type Classification - CTC

Changes to the BDAU Secure Environment or which impact BDAU SE information assets are defined into 3 categories. Approvals and testing are required as per the BDAU SE Change Management SOP. Classifications of change types are listed in the BDAU SE Information Classification SOP.

Change Platforms

Strict change types for production platforms must be enforced. Platform classifications (PC) are defined in the BDAU SE Information Classification SOP.

Introduction of New Information Assets

Introduction of new physical or electronic information assets must also abide by change type classifications unless they are automated changes, such as the introduction of new datasets or new users which are automatically provisioned.

Secure Development

All development of infrastructure software for the BDAU SE must be developed using secure and trackable code management and must be deployed using change management procedure as per the BDAU SE Change Management SOP.

Change Implementation Classification - CIC

All changes should be labelled with an appropriate change implementation classification after implementation. CICs are defined in the BDAU SE Information Classification SOP.

Version	Change
4	Relinked BDAU SE Change Management SOP Fixed Document Type
5	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
6	Modified IAM/IAO to IAO/IAA as per access control, assset management and business continuity policies Changed environment to platform as per the information classification sop
7	Reviewed: no major changes
8	Removed "As of Q4, 2019 all IAOs must be substantial employees of the College, and will be required to sign asset owner agreements." as it has not been enforced yet.

BDAU SE Corrective And Preventative Action Policy

Document Number	75451661
DR Document Number	75451657
Content Approval	See comments for version / approver
Version Number	11
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	Policy
Last Modified Date	Nov 18, 2021 16:24

This document is the Corrective And Preventative Action Policy. It describes the Big Data and Analytical Unit (BDAU) policy for addressing non-conformance and risk issues within the BDAU Secure Environment (SE).

Scope

This policy covers information assets and equipment operational within the BDAU SE as well as BDAU SE user and staff activity related to those assets and equipment. For a list of qualifying assets see the BDAU SE Asset Registry SOP. For a list of legal and regulatory requirements which we operate by see the BDAU SE ISMS Manual.

Responsibilities

Within the scope of this document the following responsibilities apply:

1. Information Security Manager (ISM) - The ISM has overall responsibility for information governance and security within the BDAU SE. The post holder is responsible for the management of Information Security Policy (ISP) as per the BDAU SE ISMS Manual and ensuring the appropriate mechanisms are in place to resolve non-conformances as required to ensure service delivery and continuity.
2. Information Asset Owner (IAO) - The IAO has overall responsibility for data contracts and data management relating to one or more information assets held within the BDAU SE as indicated by the BDAU Asset Registry and maintained according to the BDAU SE Asset Registry SOP. The IAO is responsible for approving access requests for owned information assets, ensuring the use of an information asset abides by the data processing agreement or data controller requirements for their assets and for ensuring that users of an asset notify the BDAU immediately of any actual or suspected breaches as per the BDAU SE User Registration Form.
3. Information Asset Administrator (IAA) - The IAA is the day to day contact for an information asset and can coordinate activities including access approvals and asset modification requests on behalf of the IAO with IAO permission. This does not delegate the responsibilities of the IAO however and ultimately the IAO will be held accountable for any misuse of information assets as a result of asset users or administrators. The BDAU will act as the default asset administrator for all information assets if not otherwise named. The IAA can be a non-employee of the College so long as they have the permission of the IAO to be IAA.
4. BDAU SE Staff - The staff of the BDAU in regards to the BDAU SE will abide by ISP as per the BDAU SE ISMS Manual. BDAU SE staff must ensure that non-conformances are avoided and where found are recorded as per the BDAU SE Risk Registry SOP.
5. BDAU SE Users - Users of the BDAU SE or information assets held within the BDAU SE will abide by the ISP as per the BDAU SE ISMS Manual. BDAU SE users must ensure that non-conformances are avoided and where found are raised to BDAU SE staff as soon as possible.

Non-conformity Identification

Non-conformities in the context of the BDAU SE are failures to adhere to policies and procedures as defined and linked to the BDAU SE ISMS Manual. This can include risks which are not explicitly covered by documentation but still present a risk to service delivery, security and continuity. Identification of non-conformities can be done by any user of the BDAU SE including end-users, staff and management. Suspected and confirmed non-conformities must be reported to BDAU SE staff immediately by contacting bdau@imperial.ac.uk. Non-conformities may be reported in an informal BDAU meeting for the BDAU SE staff and management. Failure to report non-conformities as detected could result in disciplinary action if required, no matter how minor the non-conformity might be. **Note that non-conformities include behaviour of other users which does not adhere to policy and procedure as defined by BDAU SE documentation.** Where identified though audit, reporting, monitoring and/or occurrence the BDAU SE staff will apply CAPA as defined below to mitigate impact and prevent recurrence.

CAPA

Corrective and preventative action (CAPA) is a systematic process of investigating, mitigating and preventing non-conformities within the BDAU SE. CAPA applies to events which have already occurred or might occur in the future. All instances of non-conformities should be referred to the BDAU SE staff for CAPA. BDAU SE staff will, along with the reporter of the non-conformity, fill in the BDAU SE CAPA Form.docx (for non-major nonconformities, save email trails instead and for preventive risks no form is needed) and add the non-conformity as per the BDAU SE Risk Registry SOP.

Corrective Action

When a non-conformity is identified the BDAU SE staff shall:

- Ensure that any remedial is taken immediately to ensure mitigation of impact of the non-conformity. This could include, for the very highest level non-conformities, cessation of service until the non-conformity no longer represents an immediate risk. For low level non-conformities this could include removal of access to a particular individual or a particular asset.
- Ensure that changes required to remove the non-conformity abide by the BDAU SE Change Management Policy where required to ensure that further non-conformities are not accidentally introduced into the BDAU SE.

Preventative Action

In order to prevent future non-conformities before they happen the BDAU SE staff and users shall:

- Attend training to ensure that policies and procedures for the BDAU SE are clear and followed as required.
- Abide by the BDAU SE Change Management Policy to ensure that non-conformities are not introduced by accident.
- Assess and explore suspected risks in an open and transparent manner.

Version	Change
7	Updated IAM/IAO - IAO/IAA as per all other policies
8	Reviewed: no major changes
9	Removed "As of Q4, 2019 all IAOs must be substantial employees of the College, and will be required to sign asset owner agreements." as it has not been enforced yet.
10	Added: 'Non-conformities may be reported in an informal BDAU meeting for the BDAU SE staff and management.' to section 'Non-conformity Identification'
11	Added to corrective action

BDAU SE ISMS Manual

Document Number	75439730
DR Document Number	75439593
Content Approval	See comments for version / approver
Version Number	22
Previous Active Version Number	21
Review Cycle (months)	12
Document Type	Manual
Last Modified Date	Feb 21, 2020 15:25

This document is the Information Security Management System (ISMS) manual. It describes the responsibilities and scope of security within the Big Data and Analytical Unit (BDAU) Secure Environment (SE).

Responsibilities

1. It is the responsibility of the Information Security Manager (ISM) to ensure that this document is up to date and relevant and reflects the scope of the ISMS. The ISM will see and obtain certification from the selected certification body.
2. A key objective of the BDAU SE ISMS Manual is to demonstrate that it takes information security seriously for the protection of our services and that of our customers and clients. The BDAU is responsible for providing and maintaining the IT systems and services for the BDAU SE, its staff, its clients and its partners that requires careful handling of information and granting access to and monitoring access tot he BDAU SE's information systems and networks.

Management Statement

1. The function of the BDAU SE is to provide data and compute services to researchers and partners as required by research programmes and processing agreements related to clinical research and advanced analytical techniques. The data provided by the BDAU and processed within the

BDAU SE is highly sensitive data. As such, the secure processing of sensitive data is a fundamental requirement for the BDAU SE. The BDAU, its staff, its clients and its partners expect our information systems to meet high standards of confidentiality, availability and integrity. These standards can only be achieved by ensuring that we have a practical and pro-active system for managing our information security.

2. This document has been approved by the Information Security Management Forum (ISMF) and gives the structure and outline of how the BDAU will set up and manage its ISMS in relation to the BDAU SE. The ISMS will contain the policies, standards, procedures, guidelines, hardware, software and other material required to manage information security within the BDAU SE. The ISMF has delegated responsibility for the establishment of the ISMS to the ISM.
3. The BDAU has established and will maintain the ISMF which made up of representation from the BDAU, its clients and its partners. The forum will approve policies and oversee the ISMS.
4. The ISMS and the security controls we apply to the BDAU SE will be based on the ISO 27001 standard and controls.
5. The BDAU is committed to meeting or exceeding its ISMS objectives and regulatory and legal obligations in regards to the BDAU SE. We will continue to develop the information security that is in place through continuous improvement of technology, policy and procedure. To this end our staff will use the documented controls and procedures in the operations of the BDAU SE to ensure that the requirements laid out in this system and in our contracts are met.
6. The BDAU will ensure that the information security requirements of any existing or future systems within the BDAU SE are defined as part of the project definition using the approved BDAU SE Onboarding SOP. These requirements will be built into our systems and maintained to ensure we can demonstrate to our clients and auditors that appropriate levels of security are in place for the BDAU SE.
7. To protect our staff and the assets of the BDAU SE, the BDAU will continue to implement our physical security procedures which include the monitoring of visitors and the provision of secure areas where required. Where services are provided by a vendor external to the BDAU a memorandum of understanding (MoU) shall be in place to ensure that services are provided to meet ISO 27001 standards and the controls required by that standard in regards to services provided for the purpose of the BDAU SE.
8. The BDAU is committed to putting in place systems that will ensure that our staff can carry out their roles in a safe and secure environment. Therefore the BDAU will uphold the policies put in place by Imperial College London in regards to appropriate use of key information and communication systems such as e-mail, telephones and the internet. We will support this policy in the BDAU SE through the implementation of controls and monitoring in accordance with documentation and legislation.
9. The BDAU, its staff, its clients and its partners will be encouraged by their line managers and through security training to think about the security of the BDAU SE and submit any questions or suggestions to the ISM.
10. The BDAU will manage the ISO 27001 ISMS in accordance with documentation under BDAU SE, with draft documentation being stored in BDAU SE Document Review.

Information Security Policy

1. The purpose of the Information Security Policy (ISP) is to protect the BDAU, its staff, its clients and its partners from all information security threats, whether internal or external, deliberate or accidental.
2. The ISP is in relation to the BDAU SE and is characterised here as the preservation of:
    a. Confidentiality - ensuring that information is accessible only to those authorised to have access
    b. Integrity - safeguarding the accuracy and completeness of information and processing methods
    c. Availability - ensuring that authorised users have access to information and associated assets when required
3. The BDAU will provide an ISM function to introduce and maintain policies and to provide advice and guidance on its implementation.
4. The BDAU requires that all breaches within the BDAU SE of information security, either actual or suspected, will be reported and investigated by the ISM.
5. The BDAU undertakes activities to provide appropriate information security awareness for its staff, its clients and its partners as appropriate in relation to the BDAU SE.
6. Third parties are required to ensure that the confidentiality, integrity, availability and regulatory requirements of systems for the BDAU SE are met as described in assigned MoUs.
7. The BDAU will hold departmental heads or other nominated managers directly responsible for implementing the policy and for the adherence of their staff and third party suppliers.
8. It is the responsibility of all personnel to adhere to the ISP.
9. The ISP shall be reviewed annually by the ISM to ensure its continued improvement.

Principles

1. This document contains both policy and procedure statements. For the avoidance of confusion, the policy statements say what we do to ensure security and the procedures give general guidance how we will implement security controls in the BDAU SE in order to meet ISO 27001 specifications. This document is used in conjunction with all BDAU SE policy and procedure documents and enforced for third party providers through MoUs.
2. The BDAU maintains a proactive approach to security in the BDAU SE to ensure risks are reduced or removed before they can damage our clients, our partners, our staff or our reputation. In implementing security, the BDAU will adopt the following principles:
    a. Integral Security - Security for the BDAU SE will be an integral part of our culture and working practices and be applied to all projects and working methods.
    b. Justified Security - Security for the BDAU SE will be justified will relation to contractual, regulatory or legal responsibilities or on the basis of risks to the business, balanced against effectiveness and cost.
    c. Manageable Security - Information security controls and solutions for the BDAU SE will be selected if they are effective, achievable, and sustainable and can be appropriately managed. Controls will be selected and implemented in a manner that ensures the minimum level of disruption to the users of the BDAU SE information processing systems and resources, both during initial implementation and through on-going usage of the systems.
    d. People are Essential - The competency of individual users of our systems is critical to maintaining information security for the BDAU SE. The BDAU therefore undertakes to train and educate its staff, its clients and its partners in their roles and to monitor their effectiveness in maintaining information security.

Scope

1. This ISMS will apply to the BDAU SE, its staff, its clients and its partners.

2. The scope of the ISMS will include all assets owned, leased, or managed by the BDAU within the BDAU SE and all means of access to information and transfer of information held within the BDAU SE. This includes all data and compute resources managed or provided by the BDAU SE.
3. The scope addresses the acquisition, handling, processing, storage and communication of information within the BDAU SE.
4. The relevant services provided by the BDAU for the BDAU SE will be defined by policies, procedures, manuals and MoUs which constitute the documentation of the BDAU SE for ISO 27001 specifications. These documents will define the appropriate security requirements for the services provided by the BDAU in relation to the BDAU SE.

Organisation Scope

1. This policy applies to:
    a. All personnel who work for or are contracted to work for the BDAU with relation to the BDAU SE.
    b. All information assets and compute resources provided or managed by the BDAU for the purposes of the BDAU SE; encompassing facilities, data, software, paper documents, and personnel where applicable.
2. Facilities include all equipment as well as the physical infrastructure for the BDAU SE:
    a. Computer processors of any size whether general or special purpose and including personal computers.
    b. Peripheral, workstation and terminal equipment.
3. Data includes:
    a. Electronic data files, regardless of their storage media and including hard copies and data otherwise in transit.
    b. Information derived from processing data, regardless of the storage or presentation media.
4. Software includes locally developed programs and those acquired from external sources:
    a. Operating system software and associated utility and support programs.
    b. Application enabling software, including database management, user management and distribution list control.
    c. Application software.
5. Paper documents including systems documentation, user manuals, business continuity plans, contracts, guidelines and procedures.
6. Personnel within the BDAU who work on or within the BDAU SE, including employees, consultants and service providers.

Key Business Processes and Functions

1. Data acquisition:
    a. Negotiation and signing of data sharing/processing agreements with relation to information assets held within the BDAU SE.
    b. Data retrieval and storage for dissemination within the BDAU SE.
2. Data provision:
    a. Acceptable usage agreements with BDAU clients and partners for the BDAU SE.
    b. Secure access to data as provisioned within the BDAU SE.
3. User management:
    a. Ensuring users have access as required for the BDAU SE according to the BDAU SE Access Control Policy.
    b. Ensuring users are removed from BDAU SE systems when applicable (leavers).
4. Compute resources:
    a. Sustained access to shared compute resources within the BDAU SE where required.
    b. Ensuring security of shared compute resources within the BDAU SE.
5. Portfolio, programme and project management:
    a. Programme management of interrelated projects to deliver organisational objectives for the purposes of maintaining and improving the BDAU SE.
    b. Portfolio management of programmes.
6. Information management and quality assurance:
    a. Management and use of data within the BDAU SE and during transfer in or out of the BDAU SE.
    b. Data protection in relation to the BDAU SE.
    c. Freedom of information in relation to the operation of the BDAU SE.
    d. IT security policy and guidance for the BDAU SE.
    e. Physical security of equipment for the BDAU SE both provided by the BDAU and by external service providers through MoUs.
    f. Change control and media management for the BDAU SE both provided by the BDAU and by external service providers through MoUs.

Personnel

1. The scope of this policy in relation to personnel applies to:
    a. The staff of the BDAU who operate within the BDAU SE.
    b. Any persons temporarily authorised for privileged access in the BDAU SE.

Interested Parties

1. The scope of this policy in relation to interested parties applies to:
    a. Registered users of the BDAU SE.
    b. Management of the BDAU including parent organisation management.
    c. Suppliers of information assets within the BDAU SE.
    d. Service providers for the BDAU SE as described by relevant MoUs.
    e. Auditors of the BDAU SE.

Information Assets

1. Information assets for the BDAU SE include security documentation, logs such as network logs and incident logs, project documents and reputation. The provision and maintenance of assets such as computer hardware and software is managed either by the BDAU or by external service providers under MoU or by both. The building is managed by Imperial College site management or by Imperial College Healthcare Trust site management.
2. Information assets are tracked in the BDAU SE Asset Registry SOP.
3. The central Imperial College Information, Communications and Technology (ICT) department provide BDAU staff workstations and operating systems for those workstations. The Imperial College ICT is also responsible for networks connecting workstations to other internal and external networks. The BDAU uses encryption for all assets within the BDAU SE including networked communication.
4. The central Imperial College ICT provides a support function, remote access facilities (Secure Gateway) and security controls (e.g. anti-virus for BDAU staff workstations and firewalls for BDAU SE networks).

Physical Environment

1. The scope of this policy in relation to physical environments applies to:
    a. BDAU staff rooms (pin code locked).
    b. Immediate locations of BDAU SE server equipment up to including the first badge protected room.
    c. BDAU SE data transfer workstation rooms.

Supporting Business Processes

1. The effective security management of the service functions of the BDAU SE is dependent on several services provided by external parties to the BDAU (including Imperial College itself). The following interfaces exist with areas in scope for services provided for the BDAU SE and these services are provided under relevant MoUs:
    a. Imperial College Human Resources (BDAU SE HR MoU)
    b. Imperial College ICT (BDAU SE ICT MoU)
    c. Internal Auditors (BDAU SE Internal Auditor MoU)
2. MoUs exist to define relevant controls for ISO 27001 specifications which these external providers adhere to for the purposes of the BDAU SE.
3. A key element of these MoUs will be the right to carry out independent audits of the service providers against the definition of the expected services defined in the MoU in relation to the on-going operational compliance of the BDAU SE. This will include documentary evidence (records or logs in either electronic or hardcopy format), which can be provided as requested at agreed intervals defined in the relevant MoU.
4. Beyond obtaining assurance for the ISMS that the relevant services defined within the MoUs are being provided correctly, there is no claim being made about the compliance of any of the service providers with respect to ISO 27001. Therefore, although clearly desirable, it is not necessary for the activities of service providers for the BDAU SE to be supported by documented policies or standards except as defined within the relevant MoU. It is also not necessary for the functions provided by these service providers to be compliant with any other clauses of ISO 27001 beyond those that have been specifically defined in the relevant MoU.

Legislative Framework

1. The legislative and regulatory frameworks which may impact particular activities within the BDAU SE include, but are not limited to:
    a. Data Protection Act (DPA) 2018 (the BDAU belongs to Imperial College and the Imperial College DPA registration number is Z5940050)
    b. General Data Protection Regulation (GDPR)
    c. Human Rights Act 1998
    d. Regulation of Investigatory Powers Act 2000
    e. The Freedom of Information Act 2000
    f. Electronic Communications Act 2000
    g. Computer Misuse Act 1990
    h. Copyright, Designs and Patents Act 1988
    i. Copyright (Computer Programs) Regulations 1992
    j. The Terrorism Act 2000
    k. Anti-terrorism, Crime and Security Act 2001
    l. Police and Criminal Evidence Act 1984
    m. Trademarks Act 1994
    n. Defamation Act 1996
    o. Official Secrets Act 1911 - 1989
    p. Obscene Publications Act 1994

Security Principles

1. There are nine general principles that provide guidance in the security of information within the BDAU SE. These are:
    a. Accountability - the responsibility and accountability of information/data owners, users and other parties concerned with the security of information should be explicit.
    b. Awareness - to foster confidence in information systems, owners, providers and users shall have access to all documentation about information security policies and procedures except where restricted by explicit requirements of non-disclosure agreements, confidentiality agreements or data sharing and processing agreements for information assets.
    c. Ethics - in the provision of information systems, information assets and the establishment of information security, the rights and legitimate interests of the BDAU's staff, its clients and its partners shall be respected.
    d. Service perspectives - security processes shall take account of and address the relevant service considerations and viewpoints; these include technical, administrative, organisational, operational, political, and legal/statutory aspects.
    e. Proportionality - the level and cost of security processes shall be appropriate and proportionate to the value and degree of resilience on information systems and the severity, probability and extent of potential or actual harm to the organisation.
    f. Integration - security processes shall be co-ordinated and integrated with each other and with other measures, procedures and practices of the organisation to create a coherent system of information security whenever possible.
    g. Timeliness - action to respond to an information security breach shall be timely and co-ordinated to prevent and overcome the breach of security.

h. Reassessment - the security of information systems shall be reassessed at times of major change and at project conception.
i. Freedom of information:
    i. The security of information will be compatible with the legitimate use and flow of data and information as required by privacy and freedom of information statutory requirements.
    ii. The BDAU in relation to the BDAU SE will follow the obligations within these guidelines to maintain best practice in information security management.

Risk Management

1. Information security controls for the BDAU SE which have been selected for implementation have been selected based on the results of a formal risk assessment to ensure a risk mediated strategy.
2. The BDAU employs a low risk strategy and is dedicated to ensuring highest levels of confidence in the confidentiality, integrity and availability of the BDAU SE information assets and information systems.
3. To ensure the effective implementation of the risk management strategy, the BDAU undertakes activities within the BDAU SE to ensure that:
    a. There are nominated individuals who shall own collectively the risk management process and lead on risk management.
    b. Risk management policies, and the benefits of following them, shall be clearly communicated to all staff.
    c. An organisational culture that supports well thought-through risk taking and innovation shall be encouraged.
    d. The management of risk is fully embedded in management processes and consistently applied.
    e. Risks associated when working with other organisations are explicitly assessed and managed.
    f. Information security risks are actively monitored and reviewed regularly on a constructive 'no-blame' basis.
    g. Audits for the BDAU SE are performed on an annual basis by external auditors who do not control access to resources held within the BDAU SE.
4. Risks are assessed using facilitated, qualitative approaches as detailed in the policies and procedures for the BDAU SE.
5. The risk assessment shall be repeated yearly as part of the ISMS review process to ensure that controls remain appropriate and adequate despite any changes of technology or vulnerabilities.

Service Continuity Strategy

1. Service continuity management is an on-going process of risk assessment and management with the purpose of ensuring that the BDAU SE can continue if risks materialise. These risks could be from the external environment, such as power failures or from within the organisation, such as deliberate or accidental damage to systems.
2. Service continuity is not just concerned with disaster recovery; it addresses anything that could affect the continuity of service over the long term.
3. Service continuity shall form an integral part of the BDAU SE ISMS and is subject to regular reviews.
4. Service continuity shall be managed in accordance with the BDAU SE Risk Register.
5. Ultimate responsibility for the information and its security rests with the ISMF who has delegated responsibility for the development, definition and management of the ISMS to the ISM. The ISM or his/her deputy chairs the ISMF.
6. The ISMF owns all documentation relating to the development, definition, and management of the ISMS.
7. Day to day management of the ISMS is vested in the ISM. The ISM ensures that all aspects of the policies are in place and that the security controls are being managed and used correctly. The ISM is the focal point for security and the ISM will seek to continuously improve security. The ISM will recommend to the ISMF security improvement plans as required.
8. The Information Security Audit (ISA) function will be provided by external auditors who will report findings to the ISMF to ensure compliance.

Responsibilities

All BDAU Staff

1. All BDAU staff are required to read and familiarize themselves with the content of the BDAU SE policies and procedures
2. All BDAU staff are required to complete training assigned to users (security awareness/regulatory training)

Senior Management

1. The Director of the BDAU and senior management of the BDAU and its parent organisation are responsible for maintaining a suitable level of security within the BDAU SE to meet our legal, contractual and regulatory responsibilities. They will select an ISM.

ISMF

1. Within the BDAU SE the ISMS will be owned and operated by the ISMF which will consist of:

Role	Responsibility
Information Security Manager (ISM)	Primary security lead for the BDAU SE
Quality Manager (QM)	Ensure quality of process, procedure and documentation
Data Officer (DO)	Representative of data vendor requirements
HR Representative	Ensures that HR MoU meets BDAU SE requirements
ICT Representative	Ensures that ICT MoU meets BDAU SE requirements

User Representative	Ensures that BDAU SE meets user requirements

2. The ISMF will have the following responsibilities:
    a. To be responsible for information security within the BDAU SE.
    b. To meet at least annually to monitor the security of the BDAU SE.
    c. To own the BDAU SE ISMS manual and the service continuity planning.
    d. To ensure that information security is covered to an appropriate level in all BDAU SE documentation and MoUs.
    e. To ensure that audits are done in accordance with the BDAU SE and that any action points raised are acted upon.
    f. To oversee and provide management guidance of security incidents.
3. The ISMF will:
    a. Nominate an ISM.
    b. Approve security policies and procedures (as necessary) within the ISM.
    c. Define specific roles and responsibilities for information security within the BDAU SE.
    d. Approve information security plans and monitor their implementation.
    e. Promote information security awareness and training within the BDAU SE.

External Service Providers

1. The BDAU holds MoUs with external service providers including Imperial College services such as HR and ICT. A full list of MoUs is maintained at BDAU SE MoU Documents.

ISM

1. The ISM will report to the ISMF. The ISM is responsible for day to day management of security within BDAU SE and for the defining, auditing and ensuring responsibility of the ISP.
2. Key responsibilities of the ISM are as follows:
    a. To monitor and report on exposure to threats to the information assets within the BDAU SE.
    b. To agree the security requirements for any system, connection to any system or any connection from any system within the BDAU SE and to audit their implementation and use.
    c. To ensure that all systems within the BDAU SE are assessed and reviewed for service risks in a manner complying with the ISMF approved risk assessment and risk management approach.
    d. Ensure the implementation of security on all BDAU SE systems is reviewed as required.
    e. To ensure all line managers, systems administrators and other staff, suppliers, contractors and other users of the BDAU SE are aware of their information security responsibilities and how to adhere to them.
    f. To provide a focus for best practice and to ensure in house security knowledge and experience are maximised within the BDAU, its staff, tis clients and its partners in regards to the BDAU SE.
    g. To review the ISMS manual on an annual basis.
    h. To identify, manage, review and monitor any security incidents for the BDAU SE and to report to the ISMF any such information security breaches.
    i. To ensure compliance with external training requirements and updates to external contracts and regulations.

Information Asset Owners

1. Information Asset Owners (IAOs) are responsible, under the direction and guidance of the ISM, for implementing the ISP for their assets, and for adherence to the ISP by asset users. Within each section each IAO will be responsible for:
    a. Ownership of systems and information identified as being owned by them within the risk assessment under Information Asset Ownership (IAO). See the ISM for details of ownership. This entails ensuring that:
        i. Information owned by the IAO is held in a manner which provides a suitable level of risk management. The risk score will be gauged against the labels identified within the BDAU SE Information Classification SOP.
        ii. Information owned by the IAO is held in a manner which provides a suitable level of integrity. The integrity of the information will be met by ensuring that the human and electronic processes are provided to reduce the risk to damage its integrity.
        iii. Information owned by the IAO is held in a manner which provides a suitable level of availability. The availability of information services will be described by the BDAU SE Business Continuity Policy.
    b. Authorisation of their staff for levels of access to the systems and revocation of those rights when they no longer require the BDAU SE (leavers, movers).
    c. Ensure that staff and contractors:
        i. Only have physical access to the areas that they need.
        ii. Only have access to the systems that they need.
        iii. Have confidentiality agreements in place where appropriate.
    d. Ensure that user IDs and passwords are assigned individually so that users may be held accountable for their actions where appropriate.
    e. Ensure that access rights are revoked when an employee leaves.

System Administrators

1. System administrators are responsible for ensuring that the systems within the BDAU SE:
    a. Maintain the security controls required for ISO 27001.
    b. Comply with the auditing policy.
    c. Are configured securely depending on the systems, known vulnerabilities and patches and accepted risks.
    d. Inform the ISM of anything that does not comply with BDAU SE requirements.

Development and Project Staff

1. Development and project staff are responsible for ensuring that all development and changes within the BDAU SE adhere to BDAU SE policies, procedures and MoUs.

All Users

1. Users of the BDAU SE systems include permanent and temporary employees, contractors, consultants, agency staff, client staff and partners who use the BDAU SE for any reason.
2. All users of the BDAU SE will be informed of their responsibilities by:
    a. Receiving and signing of the BDAU SE User Registration Form which will list their responsibilities.
    b. Receiving and signing of the BDAU SE Dataset Registration Form where applicable.
    c. BDAU SE security awareness training and certification (users).
3. All staff who service the BDAU SE will be informed of their responsibilities by:
    a. BDAU SE security awareness training and certification (staff).
4. All users and staff of the BDAU SE will be required to report all suspected or actual information security breaches to the ISM or appropriate person as soon as they become aware of them.

Management Review and Audit

Responsibilities for Audit

1. Responsibilities for management review of the suitability and effectiveness of the ISMS lies with the ISMF and will take place throughout the year.
2. The management review meeting will take place once a year.
3. Registration and evaluation documents will require 2 signatures from BDAU members and MoUs must be duly authorised by the ISM and an equivalent party for the service provider.
4. Internal audits where possible cannot be carried out by those auditing their own process and procedures.
5. External audits will require 2 signatures from BDAU members.
6. All changes to BDAU SE documentation cannot be self-authorised for publication by the drafter of the documentation.

Measuring the Effectiveness of the ISMS

1. On-going measurement of the effectiveness of the ISMS shall be achieved through the approach identified within the BDAU SE Document Control SOP.

Document and Change Control

1. All documentation relating to the ISMS for the BDAU SE shall be controlled as detailed in the BDAU SE Document Control SOP.
2. The distribution of standard documents shall be controlled and recorded using Imperial College Wiki (wiki.imperial.ac.uk) which allows for current issue status and amendment history. The distribution lists will be reviewed and updated as changes occur.
3. All changes to documents are to be reviewed and approved by the QM before issuing, and where appropriate, the nature of the change will be added on the document. Master copies of the revised documents are to be retained as records of the changes and renewed as necessary to ensure clarity.

Version	Change
18	Relinked BDAU SE Document Control SOP
19	Added Interested Parties Move scope applying to 3rd parties under Personnel to Interested Parties (previous 2b) Added new 2b for Personnel for users temporarily assigned privileged access in the BDAU SE Change table only tracks last 5 changes Changed section for BDAU to undergo staff induction to staff training (as staff induction sop is not complete yet)
20	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
21	Updated links to documentation Removed Confidential Waste MoU as there isn't one, one might need to be created, to confirm

	Updated DPA to 2018 from 1998 Added GDPR to legislation Updated BDAU staff responsibilities as there is no BDAU staff specific training Corrected ISMF meetings from bi-annually to annually, last held May 2018, next due May 2019 Updated line managers to Information Asset Owners (IAOs)`
22	Reviewed: no major changes

BDAU SE MoU Documents

This directory contains all BDAU SE memorandum of understanding documentation as per below:

- BDAU SE HR MoU
- BDAU SE ICT MoU
- BDAU SE Internal Auditor MoU

BDAU SE HR MoU

Document Number	75441887
DR Document Number	75439564
Content Approval	See comments for version / approver
Version Number	22
Previous Active Version Number	21
Review Cycle (months)	12
Document Type	MoU
Last Modified Date	Feb 03, 2022 11:23

This document represents a memorandum of understanding for services provided

to: Imperial College Big Data and Analytical Unit (BDAU)

by: Imperial College London Human Resources (HR)

in regards to the scope

of: the BDAU Secure Environment (SE)

Memorandum of understanding:

This document represents an acknowledgement by HR to provide services as described below for the BDAU. An attached copy of the live document will contain signatures of representatives of both parties. This document is part of the BDAU SE ISO 27001 certification. HR agrees to provide the services to BDAU within the scope of the BDAU SE requirements as described for each section below.

Background Checks

HR hereby declares that it does perform background checks on employees as required within the employment of Imperial College London. HR will also perform disclosure and barring service (DBS) checks where appropriate. HR will provide to the Director of the BDAU as requested, the date and status of employees in regards to passing or failing such background and DBS checks.

HR Representative Initials _____

Employee Security Responsibilities

HR requires that employees that work for or provide services to Imperial College as well as registered users of the BDAU SE abide by the following Imperial College requirements:

System Security Policy as described in http://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/

Data Quality Policy as described in https://www.imperial.ac.uk/admin-services/secretariat/college-governance/charters/policies-regulations-and-codes-of-practice/data-quality-policy/

Data Protection Policy as described in https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/our-policy/

Additionally HR acknowledges that BDAU security policies for staff as described in BDAU SE ISO 27001 policy and procedures shall also apply to employees of the BDAU within the BDAU SE.

HR Representative Initials _____

Investigations

HR acknowledges that failure of employees of the BDAU and/or registered users of the BDAU SE to comply with the policies in the previous section and BDAU SE ISO 27001 policies and procedures shall constitute a possible breach of agreement and will investigate if requested by the Director of the BDAU. Requests for investigations should be accompanied by a valid BDAU SE CAPA Form completed as per the BDAU SE Risk Registry SOP.

HR Representative Initials _____

Disciplinary Action

Imperial College requires that all management and staff adhere to Imperial Expectations as described in https://www.imperial.ac.uk/human-resources/imperial-expectations/. HR acknowledges that actions which are deemed to require disciplinary action will be investigated according to the Imperial College disciplinary process as described in https://www.imperial.ac.uk/human-resources/procedures/disciplinary/. HR accepts responsibility as required to invoke investigation as requested for employees of the BDAU and registered users of the BDAU SE at the request of the Directory of the BDAU SE. Requests for disciplinary action should be accompanied by a valid BDAU SE CAPA Form completed as per the BDAU SE Risk Registry SOP.

HR Representative Initials _____

Non-disclosure and Confidentiality

HR acknowledges that all employees of the BDAU and registered users of the BDAU SE will apply by the following Imperial College requirements:

Intellectual Property Policy as described in http://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/freedom-of-information/pulication-scheme-docs/Intellectual-Property-Policy-%5bpdf%5d.pdf

Research integrity as described in https://www.imperial.ac.uk/research-and-innovation/about-imperial-research/research-integrity/

HR also acknowledges that all employees of the BDAU and registered users of the BDAU SE will also abide by any non-disclosure agreements and/or confidentiality agreements until stated termination dates of agreements regardless of current employment, contract or student status unless otherwise explicitly stated in the relevant agreements.

HR Representative Initials _____

This agreement is duly noted by both parties as represented by the signatures below:

Printed Name	Position	Date	Signature
Mahsa Mazidi	BDAU Head of Data Management		
Christina Emmanuel	HR Staff Hub Manager		

Version	Change
18	Reviewed: no major changes Added: version/last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
19	Removed version, moved last modified
20	Reviewed: no major changes Added: version/last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes

21	Modified: Name of the Directort of the BDAU
22	Updated links and the signees

BDAU SE ICT MoU

Document Number	75444872
DR Document Number	75443557
Content Approval	See comments for version / approver
Version Number	12
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	MoU
Last Modified Date	Feb 19, 2020 16:47

This document represents a memorandum of understanding for services provided

to: Imperial College Big Data and Analytical Unit (BDAU)

by: Imperial College Information Communications and Technology (ICT)

in regards to the scope

of: the BDAU Secure Environment (SE)

Memorandum of understanding:

This document represents an acknowledgement by ICT to provide services as described below for the BDAU. An attached copy of the live document will contain signatures of representatives of both parties. This document is part of the BDAU SE ISO 27001 certification. ICT agrees to provide the services to BDAU within the scope of the BDAU SE requirements as described for each section below. Note that all references to hardware are physical, BDAU SE ISO 27001 will not apply to virtual machines as provided by ICT and these will not be part of the BDAU SE.

Network Security

The ICT manages all networks on which BDAU SE infrastructure and BDAU SE staff workstations operate. Although the BDAU SE assets are required to be encrypted and transferred securely where required as per the BDAU SE Asset Management Policy, the ICT will take the necessary steps to protect against abuse and intrusion of ICT owned networks and infrastructure. For more information see https://www. imperial.ac.uk/admin-services/ict/self-service/connect-communicate/wifi-and-networks/network-infrastructure/.

- The ICT is responsible for security of the Imperial College Secure Gateway, only users registered as per the BDAU SE User Registration SOP and allowed access as per the BDAU SE Access Control Policy will be able to access the BDAU SE via the Imperial College Secure Gateway.
- The ICT is responsible for ensuring that ICT owned networks, network devices and any other network requirements are secure from unauthorised access.
- The BDAU SE staff are responsible for local firewall management on BDAU SE servers.

ICT Representative Initials _____

Secure Areas

The ICT is responsible for ensuring that secure areas related to BDAU SE datacentre requirements is protected against unauthorised access. This is maintained by Virtus Data Centres. This includes secure loading areas for IT equipment, transfer of backup tapes to archive, hardware maintenancee. The ICT Datacentre Room Policy (available on request) applies to full and part time employees, contractors, vendors, consultants and all external visitors who require access. Access is controlled via RFID card readers for entry and all doors are fitted with sensors to detect unauthorised or prolonged door usage.

Visitor access must be agreed in advance. Unannounced/unsupervised visitors will be denied access. Closed Circuit Television (CCTV) monitoring and recording is in operation at all entry and exit points to secure areas and is centrally monitored by Virtus Security. BDAU SE equipment will reside in top-level secure racks within ICT's locked cages.

- The ICT is responsible for ensuring that unauthorised individuals do not have physical access to BDAU SE hardware residing in ICT operated datacentres except as required for authorised individuals to perform required maintenance.
- The ICT is responsible for providing to the BDAU SE logs of access to ICT operated datacentres where BDAU SE equipment resides if required for a BDAU SE investigation of access.

ICT Representative Initials _____

Environmental Security

The ICT will ensure that all necessary environmental security related to BDAU SE datacentre requirements is in place and operational. This includes regulation of power, air conditioning, generators, IT/communication cables, power outlets, fire alarms, security alarms and fire prevention equipment. ICT will ensure all equipment related to BDAU SE datacentre requirements is regularly tested and certified as Office Test compliant for energy and operational stability.

ICT Representative Initials _____

Backups and Tape Archives

The ICT will ensure that backups are performed as per the BDAU SE Business Continuity Management Policy. Backups are stored on two multi-drive tape libraries located within ICT operated datacentres and protected as per the Secure Areas section of this MoU. Backups are taken from the BDAU SE over secure transfer as per the BDAU SE Asset Management Policy. Backup tapes are not transferred outside of ICT operated datacentres and thus are protected as per the Secure Areas section of this MoU. Tapes are disposed of as per the Hardware and Information Disposal section of this MoU. Default retention for ICT backups is 3 months. Requests for restore are raised via the ICT ServiceNow portal.

- The ICT is responsible for full weekly backups with daily incremental backups.

ICT Representative Initials _____

Hardware and Information Disposal

ICT will ensure that disposal of redundant IT equipment is managed by the College Facilities Management department. Data destruction will be compliant with CESG standards. This includes BDAU SE staff workstations and BDAU SE infrastructure.

ICT Representative Initials _____

Workstation Provisions

ICT will provide ICT standard college workstations to BDAU SE staff for the purposes of management of the BDAU SE. These workstations will be provided with secure operating system configurations and all relevant anti-virus and operating system update software requirements.

ICT Representative Initials _____

Logs and Records

ICT will provide the BDAU SE with logs and configuration records as required for the following key systems for the BDAU SE:

- Imperial College Secure Gateway (https://secureaccess.imperial.ac.uk)
- Imperial College Wiki (https://wiki.imperial.ac.uk)
- Imperial College LDAP (logs for editing of all DL-CHP-BDAU* records)

ICT Representative Initials _____

ISMF Representation

The ICT will nominate an ICT representative to attend BDAU SE information security management forums as required (not usually more than twice a year). This representative will be responsible for reporting on issues which have or could have potential impact on the BDAU SE. This includes up-coming maintenance of ICT systems which would cause outage for the BDAU SE and security issues which have been reported to ICT which compromise the physical or electronic security of ICT systems related to the BDAU SE.

ICT Representative Initials _____

This agreement is duly noted by both parties as represented by the signatures below:

Printed Name	Position	Date	Signature
Melanie Leis	Director of the BDAU	12 Feb 2020	

Version	Change
8	Comment fix and old comment delete
9	Comment fix
10	Amend ICT MoU to remove local backup requirement as per audit of Mar 2018
11	Amended to reflect transfer of ICT Datacentre to Slough Sent to HR in pdf format for signing
12	Modified: Previous Active Version Number to 10

BDAU SE Internal Auditor MoU

Document Number	78530076
DR Document Number	78529235
Content Approval	See comments for version / approver
Version Number	11
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	MoU
Last Modified Date	Feb 28, 2020 12:26

This document represents a memorandum of understanding for services provided

to: Imperial College Big Data and Analytical Unit (BDAU)

by: ARC QMS LTD

in regards to the scope

of: the BDAU Secure Environment (SE)

Memorandum of understanding:

This document represents an acknowledgement by ARC QMS LTD to provide services as described below for the BDAU. An attached copy of the live document will contain signatures of representatives of both parties. This document is part of the BDAU SE ISO 27001 certification. ARC QMS LTD agrees to provide the services to BDAU within the scope of the BDAU SE requirements as described for each section below.

Internal Audit

ARC QMS LTD will perform internal audits on behalf of the BDAU SE staff in regards to the BDAU SE. These audits will cover specific agenda items to be drafted in advance of internal audits but will cover the following high-level items:

- Conformity with ISO standards
- Accuracy of policy and procedures
- Compliance and effectiveness of systems
- Regulatory and legislative requirements

ARCQMS Representative Initials _____

Internal Audit Report

At the end of each internal audit, ARC QMS LTD will provide a report the BDAU SE ISM containing the outcome of the internal audit with findings and recommendations for corrective actions.

ARCQMS Representative Initials _____

Non-disclosure and Confidentiality

ARC QMS LTD acknowledges that audit reports are sensitive in nature and will not disclose the agenda or outcomes of internal audits to parties other than the BDAU, it's parent organisation and ARC QMS LTD staff on a need to know basis without the express permission of the Director of the BDAU.

ARCQMS Representative Initials _____

This agreement is duly noted by both parties as represented by the signatures below:

Printed Name	Position	Date	Signature
Melanie Leis	Director of the BDAU		
Craig Lash-Hartnoll	ARC QMS LTD		

Version	Change
7	Old comment delete
8	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
9	Reviewed: no major changes
10	Modified: Name of the Directort of the BDAU Sent to ARC QMS LTD in pdf format for signing
11	Removed "Health and safety requirements" from Internal Audit section as it is not done by ARC QMS

BDAU SE Asset Registry SOP

Document Number	75442449
DR Document Number	75442446
Content Approval	See comments for version / approver
Version Number	10
Previous Active Version Number	9
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Apr 28, 2021 10:46

This document describes how to update and record assets in the BDAU SE Asset Registry stored under DS001.

Procedure

Staff Procedure

Staff are required to update the BDAU SE Asset Registry in "/data/master/DS001/extract/registries/Asset Reg.ods" as per the BDAU SE Asset Management Policy. Currently we only update the Information & Data sheet of the BDAU SE Asset Registry.

User Registry

Users are tracked by username using the BDAU SE User Registration SOP.

Information and Data Registry

Information and data assets are tracked within the BDAU SE Asset Registry using the Information & Data sheet. The fields are:

- Asset Type - One of the valid asset types covered by the BDAU SE Asset Management Policy scope. Currently we record Data, Vendor, Hardware and Software asset types.
- Asset Local ID - The local identifier for the BDAU SE for the asset. Valid identifier formats are listed for asset types below:
  - Data Asset Type - DSXXX where XXX is an unique ID as defined in the BDAU SE Dataset Evaluation SOP.
  - Vendor Asset Type - VXXX where XXX is an unique ID as defined in the BDAU SE Vendor Evaluation SOP.
  - Hardware Asset Type - HWXXX where XXX is an unique ID (taken sequentially for new assets).
  - Software Asset Type - SWXXX where XXX is an unique ID (taken sequentially for new assets).
- Asset Owner - The IAO for the asset (see BDAU SE Asset Management Policy, in most cases this is bdau@imperial.ac.uk for non dataset assets, but could also include specific project or department leads).
- Asset Admin/Project Lead - The IAA for the asset (see BDAU SE Asset Management Policy, IAA will be the primary contact for data instead of AO)
- Asset Users - The active users of this asset. Typical identifier examples are listed for asset types below:
  - Data Asset Type - dl-chp-bdau-dsXXX@imperial.ac.uk where XXX is an unique ID as defined in the BDAU SE Dataset Evaluation SOP. The users for data assets are held in these distribution lists so this doubles as both a way to contact active users, ensure they still require access as well control the access itself.
  - Vendor Asset Type - typically always bdau@imperial.ac.uk as this is a metadata asset used by the BDAU SE staff to track datasets tied to a vendor as per the BDAU SE Vendor Evaluation SOP while the BDAU SE Dataset Evaluation SOP tracks the primary contact and users at the dataset level.
  - Hardware Asset Type - typically always bdau@imeprial.ac.uk for any workstations and servers
  - Software Asset Type - typically always bdau@imeprial.ac.uk
- Asset Vendor - The vendor that provides the asset. Typical identifier examples are listed for asset types below:
  - Data Asset Type - VXXX where XXX is an unique ID as defined in the BDAU SE Vendor Evaluation SOP and assigned to the dataset during the BDAU SE Dataset Evaluation SOP.
  - Vendor Asset Type - typically always bdau@imperial.ac.uk as this is a metadata asset used by the BDAU SE staff to track datasets tied to a vendor as per the BDAU SE Vendor Evaluation SOP
  - Hardware Asset Type - ICT if provided by ICT
- Asset Vendor ID - This is the DSA, IPA, agreement ID or study protocol ID which belongs to this asset. If an agreement ID is not provided this defaults to a project summary. For hardware asset types this should be the ICT asset tag of the asset or internet protocol address.
- Asset Description - The description of this asset. Typical identifier examples are listed for asset types below:

    - Data Asset Type - DSXXX Project X - Project short summary, where DSXXX is the unique identifier as determined by the BDAU SE Dataset Evaluation SOP and Project X is the project number identifier for the project in the applicable DSA/IPA, unless one does not exist in which case it defaults to Project 1 for the primary project in that DSA/IPA.
    - Vendor Asset Type - Vendor evaluation followed by vendor name. For instance "Vendor evaluation NHS Digital". Note that the vendor is universal for both private and public data where the contact for the vendor is the same as determined by the BDAU SE Vendor Evaluation SOP.
    - Hardware Asset Type - The brief description of the machine and it's use
- Asset Expiry Date - Date the agreement/contract for the asset expires if applicable.
- Asset Destruction Date - Date the asset is destroyed or removed if applicable.

Version	Change
6	Added content required for Information and Data Registry sheet (as already being collected for the previous 3 - 4 months)
7	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
8	Added hardware asset type with required field descriptions Updated asset owner definition to match with and reference IAO from asset management policy
9	Reviewed: no major changes
10	Added Software asset, IAA, Asset Expiry and Destruction dates.

BDAU SE Bring Your Own Device/Personal Electronic Device SOP

Document Number	261097455
DR Document Number	261097447
Content Approval	See comments for version / approver
Version Number	3
Previous Active Version Number	2
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Apr 25, 2022 13:56

This document describes the use of all users' own Personal Electronic Devices (i.e. not College owned) in respect of BDAU SE related work. This SOP is in line with the College "Information Systems Security Policies", particularly the Information Security Policy.

Procedure

User Procedure

Here a Personal Electronic Device (PED) is any electronic device (such as laptop, tablet or mobile phone), owned by a BDAU SE user that is used for accessing, or facilitating access to, BDAU SE related data or communications. Such use of PEDs may also be termed Bring Your Own Device (BYOD). Note that the below requirements also apply to College owned equipment used for the same or similar purposes (it may be that College ICT automatically implement some of the below as a matter of College policy).

All BDAU SE users are required to ensure that their own Personal Electronic Devices:

1) Are kept up to date with all vendors patches and security updates, including running currently supported versions of vendor operating systems and software. College ICT provide guidance.

https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/installing-updates-and-antivirus/

2) Are secured with an appropriately strong password and/or via the use of secure biometric options; device screen locking must be enabled. Appropriate here is a password or passphrase consistent with College guidance and the National Cyber Security Centre's 'Cyber Aware' advice.

https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/passwords-and-extra-security/passwords/

https://www.ncsc.gov.uk/cyberaware/home

3) Are secured with whole device encryption. Consult your device vendor's instructions as to how to achieve this. College guidance is also available.

https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/encrypt-and-protect-your-data/

https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/keeping-mobiles-and-tablets-protected/

4) Use anti-virus and similar products to curb malware and intrusion attacks. College ICT can provide specific guidance.

5) Physically secured. **If your Personal Electronic Device is lost or stolen, you must advise BDAU SE staff immediately.** You must change your College Single Sign On password right away. Please see the following SOP for more guidance: BDAU SE Loss/Compromise/Change of User Authentication Tokens SOP.

For further advice consult the College's 'Be Secure' IT security guidance:

https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/

Version	Change
1	Document creation Added DR Document Number Added Published Document Number
2	Edited title. Screen locking.
3	Fixed link to the compromise/change/loss of authentication tokens SOP, Tidy up.

BDAU SE Change Management SOP

Document Number	75446354
DR Document Number	75446351
Content Approval	See comments for version / approver
Version Number	5
Previous Active Version Number	4
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Feb 19, 2020 15:13

This document describes the procedures related to making changes within the BDAU SE which abide by the BDAU SE Change Management Policy.

Procedure

User Procedure

Users of the BDAU SE are required to adhere to the BDAU SE Change Management Policy and are not allowed to make unauthorised changes to the BDAU SE on behalf of themselves or other users. This includes installation of software such as external modules for programming languages or software packages or using pre-built software or compiled software without the express permission of the BDAU SE ISM. Failure to adhere to this requirement could result in loss of access and disciplinary action if required.

Staff Procedure

1. Classify platform of change as per the BDAU SE Information Classification SOP PC.
2. Classify change type as per the BDAU SE Information Classification SOP CTC.
3. Classify continuity requirements of affected assets as per the BDAU SE Information Classification SOP BCC.
4. Follow change procedure as per the chart at the bottom of this page:
    a. C-Dev - This change affects assets which are easily restored or not needed in the first place, follow steps as per below:
        i. Notify ISM and obtain approval (email confirmation required).
        ii. Make change and classify implementation as per the BDAU SE Information Classification SOP CIC.
    b. C-UAT - This change affects assets which are easily restored or not needed in the first place (this will be modified in future versions TODO), follow steps as per below:
        i. Notify ISM and obtain approval (email confirmation required).
        ii. Make change and classify implementation as per the BDAU SE Information Classification SOP CIC.
    c. C-Prod-BNR - This change affects assets which are easily restored or not needed in the first place (this will be modified in future versions TODO), follow steps as per below:
        i. Notify ISM and obtain approval (email confirmation required).
        ii. Make change and classify implementation as per the BDAU SE Information Classification SOP CIC.
    d. C-Prod-BP-PC - This change affects assets which are business preferred or business critical or cannot be easily restored (this will be modified in future versions (TODO), follow steps as per below:
        i. Notify ISM and obtain approval (email confirmation required).
        ii. Notify all users via email of affected asset(s) either by individual asset contact as per the BDAU SE Asset Registry SOP or the entire BDAU SE user list (DL-CHP-BDAU-SG) with no less than 2 weeks notice (unless emergency change, then post-notification is okay but only with ISM approval).
        iii. Make change and classify implementation as per the BDAU SE Information Classification SOP CIC.

Change Procedure Mappings

PC	CTC	BCC	Procedures
Development	Any	NA	C-Dev
UAT	Any	NA	C-UAT
Production	Any	Business Non-required	C-Prod-BNR

Production	Any	Business Preferred OR Business Critical	C-Prod-BP-BC

Version	Change
1	Document creation
2	Added DR Document Number Added Published Document Number
3	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
4	Added "unauthorised" even though it was already clear that users can be given permission for software installation under certain circumstances Changed environment to platform as per information classification SOP
5	Reviewed: no major changes

BDAU SE Communications SOP

Document Number	78527650
DR Document Number	78525999
Content Approval	See comments for version / approver
Version Number	10
Previous Active Version Number	7
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Feb 19, 2020 15:15

This document describes the process for communication in relation to the BDAU SE. BDAU SE users are not authorised to communicate on behalf of the BDAU.

Procedure

User Procedure

Users of the BDAU SE should contact bdau@imperial.ac.uk for all items which constitute communication in relation to the BDAU SE including but not limited to grant applications, ethics approval, data sharing agreements or any other form of internal and external communication. If the communication is in regards to the BDAU staff it should be communicated to BDAU Director (currently Leis, Melanie S), if the communication is in regards to the BDAU staff including the Director of the BDAU it should be escalated to the Director of Operations for the Centre for Health Policy (currently Fontana, Gianluca).

Staff Procedure

All communications on behalf of the BDAU or in regards to the BDAU SE should be approved by the Director of the BDAU. No person may speak on behalf of the BDAU or in regard to the BDAU SE without the explicit permission of the Director of the BDAU. Once approved all external communication should be done through the Institute for Global Health Innovation by emailing ighi@imperial.ac.uk.

For cascading issues to BDAU SE Staff use the email address bdau@imperial.ac.uk. See the BDAU SE Staff Working Areas SOP for staff relocation instructions if necessary.

Version	Change
6	Added in missing last modified date
7	Reviewed: no major changes
8	Modified: BDAU Director to Melanie Leis
9	Modified: Remove Melanie Leis from Staff Procedure
10	Reviewed: no major changes

BDAU SE Communications with the BDAU SE Users SOP

Document Number	142268256
DR Document Number	142261733
Content Approval	See comments for version / approver
Version Number	9
Previous Active Version Number	8
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	May 10, 2022 15:18

This document describes the procedures for chasing information and the process to revoke access from BDAU SE users after a certain time if repeated queries are not answered.

Procedure

User Procedure

Users of the BDAU SE should respond to communications from BDAU SE staff in a timely manner to prevent delays and interruptions in access to data. To contact the BDAU please use the email address bdau@imperial.ac.uk.

Staff Procedure

BDAU SE Staff should contact BDAU SE users using their Imperial email for chasing information (including follow up with users if they have not renewed their access in the given timeframe).

> ⚠ **For all communications, use the BDAU SE user's Imperial email address.**

1. First contact is made to the BDAU SE user.
2. If no response after two weeks, email the BDAU SE user again.
3. If no response after two weeks, email the user again including the asset owner, asset admin and the entire dl related to the specific dataset, stating next steps if no response in the given timeframe. E.g. for final message to the entire DL, add 'if you do no reply after 10 days, we will revoke access.'
4. If no response after two weeks, access to the dataset is suspended through scrambling of users' passwords.
    a. If user has an expired dataset registration and no response is received, proceed with removing user from the dataset as per the BDAU SE User Removal from a Dataset SOP (skip the first step of the SOP).
    b. If user has an expired user registration and no response is received, proceed with removing user from the BDAU SE as per the BDAU SE User Removal SOP (skip the first step of the SOP).

Additionally, when relevant, for any emails surrounding IGHI projects add Hendramoorthy Maheswaran (h.maheswaran@imperial.ac.uk), for Business School add Jack Olney (jack.olney@imperial.ac.uk) and for Department of Primary Care & Public Health (PCPH) add Mark Cunningham (mark.cunningham@imperial.ac.uk) to the CC section.

Version	Change
5	Fixed Typos
6	Modified: Changed the title of document Added Document Number
7	Reviewed: No major changes
8	Updated the contact for IGHI, added a new contact for PCPH
9	Clarified the staff procedure, formatting.

BDAU SE Conflict Of Interest SOP

Document Number	75446797
DR Document Number	75446794
Content Approval	See comments for version / approver
Version Number	7
Previous Active Version Number	6
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Apr 21, 2021 15:29

This document describes the procedures for avoiding conflicts of interest for BDAU SE staff, its clients and its partners.

Procedure

User Procedure

Users of the BDAU SE must ensure that they do not hold conflicts of interest which might inhibit their ability to lawfully make use of the BDAU SE. This could include conflicts of security such as being privileged users of ICT or conflicts of responsibility such as being information governance leads for BDAU SE vendors. If such cases arise users should seek an exception from the BDAU SE as per the BDAU SE Exception Registration SOP.

Staff Procedure

BDAU SE staff are required to adhere as much as possible to the avoidance of conflicts of interest. To help ensure this happens the following guidelines are applicable:

- When signing any document on behalf of the BDAU SE, those documents must also be signed by another member of the BDAU (in addition to the user signature if required), some examples are:
  - BDAU SE Vendor Evaluation SOP
  - BDAU SE Dataset Evaluation SOP
  - BDAU SE Dataset Registration SOP
  - BDAU SE User Registration SOP
- Internal audits where possible can not be carried out by those auditing their own process and procedure
- All changes to BDAU SE documentation should be authorised by both the drafter and another BDAU SE staff, a BDAU drafter should not self-approve documentation changes (exceptions are made for initial documentation requirements)
- Background checks will be performed on BDAU SE staff members (referenced in the BDAU SE HR MoU)

Version	Change
3	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
4	Removed BDAU signoff requirement for external auditors as external audits are performed by accredited company, currently ISOQAR
5	Modified: Changed Admin Procedure to Staff Procedure
6	Reviewed: no major changes
7	Corrected typos, added a link to the HR MoU

BDAU SE Dataset Evaluation SOP

Document Number	75442467
DR Document Number	75442351
Content Approval	See comments for version / approver
Version Number	18
Previous Active Version Number	17
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Apr 28, 2021 10:45

This document describes how to complete the BDAU SE Dataset Evaluation process for new or existing datasets. This is required in order to register users for datasets using the BDAU SE Dataset Registration SOP.

Procedure

User Procedure

1. If you wish to use a new/existing dataset within the BDAU SE environment, you need to work with the BDAU to complete the BDAU SE Dataset Evaluation Form.docx.

Staff Procedure

1. Fill out the BDAU SE Dataset Evaluation Form.docx
    a. **Dataset ID:** Next sequential dataset ID (contact bdau@imperial.ac.uk to get this from Asset Registry)
    b. **Asset Owner:** IAO as per BDAU SE Asset Management Policy
    c. **AO Training Required:** Is asset owner training required for this dataset
    d. **Asset Users:** Contact email for users of the asset (i.e. dl-chp-bdau-ds002@imperial.ac.uk)
    e. **BDAU Vendor ID:** ID of vendor as specified in the appropriate vendor evaluation form (ask bdau@imperial.ac.uk if not clear, primary are V001 for HES and V002 for CPRD)
    f. **Asset Description:** Description of asset including purposes for processing, try to be concise but clear as this will be used to determine further access for other users
    g. **Vendor Contract ID:** Contract code between College and data provider, a copy of this contract should be accessible by BDAU
    h. **Vendor Contract Expiry:** Date the contract above expires
    i. **Vendor Agreement ID:** In some cases, notably HES data agreements, data sharing agreements may differ from contracts, in the case where a separate agreement is present it should be listed here and a copy should be accessible by BDAU
    j. **Vendor Agreement Expiry:** Date the agreement above expires
    k. **Vendor Data Deletion Date:** This is the date original data must be deleted by if applicable, if in doubt set to expiry date of contract or agreement, whichever comes first
    l. **Sublicense ID (if required):** This is currently only required by CPRD for honorary contracts
    m. **Legal Basis:** The legal basis for both the collection and processing of data, primary examples are
        i. Section 251 - exception granted to hold identifiable data without patient consent
        ii. Section 261/Article 9 (2) (i/j) - exception granted to hold pseudonymised data without patient consent
        iii. GDPR Article 6 (1) (a) - consent granted to process, collect or hold data (must have public information location as per next item)
    n. **Public Information Location:** Location of privacy policy for processing of the data
    o. **Breach Notification Policy:** Explained in document, note that ISO 27001 must always be set to 1 if data is inside BDAU SE
    p. **Project Lead:** Primary contact for data instead of AO, this can be a non-substantial employee of the college, but all governance requirements and access to data requests must be approved by AO. Project Lead will be replaced by IAA as per BDAU SE Asset Management Policy in the next dataset evaluation form refresh.
    q. **Availability Class:** as per the **BDAU SE Information Classification SOP**
    r. **Information Class:** as per the **BDAU SE Information Classification SOP**
    s. **Data Re-identification:** This must be completed if not anonymised data, consider all the risks to re-identification and if risk is applicable set to 1
    t. **DPIA Required:** If availability class * information class * data re-identification is greater than 0, a College DPIA or FoM RDPIA must be completed with help from bdau@imperial.ac.uk
    u. **BDAU Reviewer:** BDAU staff member performing review
    v. **Transfer Method:** One of - https, sftp, etc... (must be a secure encyrpted transfer type, i.e. not via email or unencrypted download)
    w. **Transfer Username:** Username used to transfer data

x. **Valid From:** Date from which the data is valid
y. **Last Reviewed:** Date of review currently in progress
z. **User Restricted:** Is this dataset restricted to only particular users
aa. **Retention Period:** How many years does this dataset need to be retained
ab. **Archived:** Is this dataset still active, YES if it's non-active, i.e. it is archived

2. Once form has been completed, print out and sign
    a. **BDAU SE Authorisation:** BDAU staff member signature, printed name and signing date
    b. **BDAU SE ISM Authorisation:** BDAU ISM signature, printed name and signing date
3. Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Schema.docx
4. Save document from email to BDAU SE Dataset Evaluations directory (/data/master/DS001/extract/evaluations/datasets)
5. Add to BDAU SE Asset Registry as per the BDAU SE Asset Registry SOP

Version	Change
14	Change Previous Active Version Number
15	Change Version number
16	Reviewed: no major changes
17	Modified "Sublicense ID (if required):" item (changed "Q4, 2019" to "Q3, 2020") Modified "Project Lead" item (Changed "This will be replaced by IAA as per BDAU SE Asset Management Policy in dataset evaluation refresh by Q4, 2019" to "Project Lead will be replaced by IAA as per BDAU SE Asset Management Policy in dataset evaluation refresh by Q3, 2020.") as Project Lead was not replaced by IAA in dataset evaluation refresh in Q4, 2019.
18	Modified AO training required and Sublicense ID sections, Added a link to the FoM DPIA tool, Added signing date to authorisation step, Added alternative instruction for when processing forms remotely

BDAU SE Dataset Registration SOP

Document Number	75442474
DR Document Number	75442364
Content Approval	See comments for version / approver
Version Number	12
Previous Active Version Number	11
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Dec 11, 2020 09:36

This document describes how to complete the BDAU SE dataset registration process. This is required in order to be granted access to data within the BDAU Secure Environment. Note that the BDAU SE Dataset Evaluation SOP is required prior to the BDAU SE dataset registration process.

Procedure

User Procedure

1. The first step is to register for data using the BDAU SE Dataset Registration Form.docx. This form covers the agreement between yourself and the BDAU in regards to appropriate use of data within the BDAU SE.
    a. You will need to provide a **billing contact** email.
        i. If you are billing from PCPH this is b.cerutti@imperial.ac.uk.
        ii. If you are billing under CHEPI/Business School this will be jack.olney@imperial.ac.uk.
        iii. Any other users must provide the email of their **academic supervisor** or **line manager.**
    b. If you are registering for a new dataset, the BDAU will fill out the BDAU SE Dataset ID once the request is submitted.
2. Once this form has been completed, it can be scanned and sent to bdau@imperial.ac.uk for processing. Please note:
    a. This form is only valid until the next 31st of January.
    b. Your access will be removed automatically if you do not renew your BDAU SE Dataset Registration.
    c. By signing the agreement the BDAU SE user understands that he/she will be held liable for not following the agreement.
3. Once your access has been completed, you can access the dataset within the BDAU SE within 1 hour of access confirmation by following the BDAU SE data access guide. Form and training required in BDAU SE User Registration SOP must be completed prior to information asset access.

Staff Procedure

1. Email user the link to BDAU SE Dataset Registration SOP, ask them to follow the intructions as per the User Procedure.
2. On receipt of the completed BDAU SE Dataset Registration Form.docx, the BDAU SE staff are responsible for completing the dataset registration process using the instructions below:
    a. Sign the form (note that BDAU delegates in other business lines may also sign forms).
    b. Obtain the BDAU SE ISM signature on the form.
    c. Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Schema.docx.
    d. Save document from email to BDAU SE Dataset Registrations directory (/data/master/DS001/extract/registrations/datasets).

        ⚠ Make sure the document is named exactly as per BDAU SE Record Naming Schema.docx.

    e. Complete the procedure in the BDAU SE Data Provisioning SOP.

Version	Change
8	Modified 2b to be manual, not automatic and 1 month instead of 2 months grace period Clarified training requirements

	Changed staff procedure to reference the BDAU SE Data Provisioning SOP which contained all steps previously contained here with more detail
9	Removed: Deleted part of Step 2
10	Reviewed: no major changes Edited User Procedure - clarify expiry of BDAU SE user registration form Edited Staff Procedure: BDAU SE admin to BDAU SE staff
11	Reviewed: no major changes
12	Updated User and Staff Procedures

BDAU SE Exception Registration SOP

Document Number	75446382
DR Document Number	75446379
Content Approval	See comments for version / approver
Version Number	8
Previous Active Version Number	7
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Feb 19, 2020 15:37

This document describes when and how to obtain or grant an exception for the BDAU SE. Exceptions are granted at the sole discretion of the BDAU SE when the BDAU SE capacity cannot meet user or dataset requirements.

Procedure

User Procedure

Users who are directed to the BDAU for services provided within the BDAU SE are expected to make all reasonable attempts to work with the BDAU SE to ensure that they can make use of the BDAU SE services for as much of their data requirements as possible. In limited circumstances it is understood that the BDAU SE may not be able to provide services as required by the users. In this case an exception will be provided for the user as per the Staff Procedure section below. Users will be expected to abide by any terms and conditions of the exception which is granted especially in regard to dataset exceptions where the BDAU SE staff are assisting with best practice outside of the BDAU SE. Users cannot grant their own BDAU SE exception. All exceptions are granted for 1 year unless the user is unlikely to be working on data within Imperial College or within the BDAU SE (determined at the sole discretion of the BDAU SE ISM) in which case a 5 year exception or indefinite exception can be granted. The user should always seek to return into the BDAU SE if possible and make every reasonable attempt to work with the BDAU SE to do so.

Staff Procedure

1. Staff must first determine if an exception is actually required, this must involve the ISM. Exceptions are usually granted if:
    a. The user requires software which is NOT provided by the BDAU SE and CANNOT be installed and provided securely without significant investment of time and resources.
        i. Example - user is using macintosh only software.
        ii. Example - user is using software licensed for a single user (BDAU prefers concurrent licenses).
    b. The user does not hold or analyse ANY data within Imperial College London.
2. Staff must then classify the exception type:
    a. Step 1a - This is a Dataset Exception unless this is the only dataset which the user would use within BDAU SE jurisdiction, in which case an User Exception would be granted.
    b. Step 1b - This is an User Exception.
3. Staff must determine the length of exception required to be recommended to the BDAU SE ISM. The default is 1 year unless the exception is unlikely to be lifted or the user is not going to be within the jurisdiction of the BDAU SE, in which case a 5 year or indefinite exception can be recommended.
4. Staff must fill in the BDAU SE Dataset Exception Form or BDAU SE User Exception Form as required and pass it to the BDAU SE ISM for approval. The user must also sign this form.
5. BDAU SE Dataset Exceptions must also be filed as per the BDAU SE Asset Registry SOP.

Version	Change
4	Fixed last active version
5	Updated last active version Removed duplicate filing line
6	Reviewed: no major changes Added: last modified

	Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
7	Reviewed: no major changes
8	Reviewed: no major changes

BDAU SE Information Classification SOP

Document Number	75442458
DR Document Number	75442346
Content Approval	See comments for version / approver
Version Number	17
Previous Active Version Number	16
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 25, 2022 13:30

This document is the BDAU SE Information Classification SOP. It describes the Big Data and Analytical Unit (BDAU) procedure for classification, labelling and handling of information assets within the BDAU Secure Environment (SE).

Procedure

User Procedure

User Responsibilities

All users of the BDAU SE must abide by information classification requirements. Where information is not yet labeled users should raise this to BDAU SE staff to be labeled. Only information which is anonymised in line with ICO guidance is allowed to leave the BDAU SE without an exception.

Staff Procedure

Staff Responsibilities

All BDAU SE staff are responsible for ensuring that information is accurately labelled and handled correctly as per the BDAU SE Asset Management Policy.

Classification

The classification of information within the BDAU SE is based on perceived sensitivity of the information and an estimate of the potential risk in the event of its disclosure. The BDAU SE staff will classify information in 2 parts:

Availability Class

The legal availability of the information.

- Public - Information which is publicly available for access.
- Private - Information which is not publicly available for access.

Information Class

The sensitivity of the information.

- Publishable - Information which is for publication and contains only information which can be made public with the publisher's discretion:
    - Research output which does not contain information which cannot be made public.
    - Documentation which does not contain information which cannot be made public.
- Anonymised - Information is completely anonymised and contains no identifying data. Note that datasets which contain free-text elements are automatically classed as risk score of medium or higher depending on content unless it is labelled as publishable.
- Pseudonymised - Information which contains data which can be used to re-identify individuals.
- Identifiable - Information which can be used directly to identify individuals, this is forbidden in the BDAU SE.

Risk of Re-identification

The availability class and information class are used along with a re-identification risk assessment to determine if a College Data Protection Impact Assessment (DPIA) is required. See the BDAU SE Dataset Evaluation SOP for more information on how to label information assets.

Labelling

BDAU SE documentation published on the Imperial Wiki is considered public and publishable data and should not contain any sensitive data such as password or other information which could not be made public. However some of the BDAU SE documents published on the wiki such as access procedures, system monitoring and administration standard operating procedures are considered private and publishable with discretion of the BDAU SE ISM. BDAU SE logs, records, scanned contracts and other information (in DS001) are considered private and publishable with discretion of the BDAU SE ISM. Labelling of information is done in evaluation procedures (see BDAU SE Dataset Evaluation SOP). All information should have a label and BDAU SE staff are responsible for ensuring that this happens.

Handling

BDAU SE staff must ensure that all data is handled and disposed of as per the BDAU SE Asset Management Policy, BDAU SE Data Provisioning SOP and BDAU SE ICT MoU (disposal). All information not classified as publishable should be encrypted in transit.

Business Continuity Classification - BCC

BDAU SE staff must ensure all information asset have a business continuity classification as defined in the chart below.

BCC	Definition	Notes
Business Critical	Information assets which are critical to the functionality and on-going service of the BDAU SE, its staff and users. All information assets listed as business critical should have an associated failover and be tested for BCM testing.	Currently all assets are considered critical until Dev /UAT are ready.
Business Preferred	Information assets which are preferred for business continuity but non-critical. Information assets which are deemed business preferred should have a failover associated for production environments but do not have to pass BCM testing.	Not in use as per above.
Business Non-required	Information assets which are not required to continue business and do not require a failover resource. This would include development and UAT environments.	Not in use as per above.

Change Type Classification - CTC

BDAU SE staff must ensure all information asset changes are labelled with an appropriate change type classification as defined in the chart below.

CTC	Definition
Standard Change	A relatively low-risk change with well-understood outcomes that is made without impact to users of the BDAU SE.
Significant Change	A change that is one that has medium to high risk for critical services, involves less understood risks, has less predictable outcomes, and /or is a change that is not regularly made during the course of business.
Emergency Change	A change which is executed under circumstances of urgency, such as removal or moving of files to clear disk space.

Platform Classification - PC

BDAU SE staff must ensure all platform assets are labelled with an appropriate environment classification as defined in the chart below.

PC	Definition	Notes
Development	The development platform is a business non-required environment and should only ever require standard changes as the platform should be re-creatable relatively easily and/or has low impact for users of the BDAU SE.	Not in use as per below.
User Acceptance Testing (UAT)	The UAT platform is a business preferred platform in that it provides a continuous improvement. However, outages on the UAT platform should not have lasting impact to users and ultimately the platform can be recreated.	Not in use as per below.

Production	The production platform is a business critical platform and all CTCs must be fully applied as defined.	Currently all assets are considered production until Dev /UAT are ready.

Change Implementation Classification - CIC

BDAU SE staff must ensure all changes are labelled with an appropriate change implementation classification after implementation as defined in the chart below.

CIC	Definition
Successful	Changes to the environment went as planned and there were no negative effects on any systems.
Implemented With Issues (IWI)	Changes to environment went as planned but there were some negative effects on some systems.
Unsuccessful	Unsuccessful changes are changes which failed to deliver the benefits of the change. Unsuccessful changes should not be implemented in upstream systems.

Version	Change
13	Updated data allowed to leave Changed risk score matrix to reference dataset evaluation form Added notes to clarify that as Dev/UAT are not in use, all assets are considered critical and not in use
14	Changed environment classification to platform classification
15	Reviewed: no major changes Edited Information class
16	Reviewed: no major changes
17	Fixed the link to College DPIA, updated labelling section

BDAU SE Non-conformance SOP

Document Number	78527975
DR Document Number	78527668
Content Approval	See comments for version / approver
Version Number	11
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 25, 2022 15:41

This document describes how to raise a CAPA request for any non-conformance, including security incidents, for the BDAU SE.

Procedure

User Procedure

Users of the BDAU SE are responsible as per the BDAU SE User Registration Form.docx to raise any non-conformances including suspected security incidents to bdau@imperial.ac.uk. Failure to do so could result in loss of access and possible disciplinary action.

Staff Procedure

Upon receipt of a non-conformance or security incident report from users the BDAU SE staff are responsible to assess the issue and fill in a BDAU SE CAPA Form.docx if necessary. The purpose of this form is to create an appropriate assessment of the causes of the non-conformance and to formulate a plan to re-mediate or mitigate any existing or subsequent risk. The fields are:

- **Asset Local ID(s):** a comma separated list of asset IDs as per the BDAU SE Asset Register (see BDAU SE Asset Registry SOP). This could be hardware as well as software assets. If all datasets are affected simply list the hardware asset HW001.
- **Description:** a detailed description of the non-conformance as described by the user and investigated by staff. If more room is required, create an additional word document and name it according to the BDAU SE Record Naming Schema.docx prepended with FD_, for instance FD_BDAUSE.NC.R001.20170407.00744268. This should be scanned along with the CAPA form when saving to BDAU SE archive.
- **Raised On (date):** raised on date of the issue, i.e. the date the user sent you and email or raised it with you directly, if not known use the current date.
- **Raised By (email):** the email of the person who raised the original issue, if it is staff raised then use bdau@imperial.ac.uk.
- **BDAU SE Reviewer:** the BDAU SE staff member reviewing the event and formulating the treatment plan.
- **BDAU SE Review Date:** the date the BDAU SE staff member filled in the CAPA form or updated the most current revision.
- **BDAU SE Corrective Plan:** the plan which will be used to correct any existing impact caused by the non-conformance. This could include removing a users or staff access, rebooting the central BDAU SE or even shutting down the BDAU SE until the issue is resolved.
- **BDAU SE Prevention Plan:** the plan which will be used to prevent any future impact caused by the non-conformance. This could include removing a users or staff access permanently, removing access to particular software or data asset or shutting down the BDAU SE until the issue is resolved.
- **BDAU SE Reviewer Signature:** the signature of the staff member who last reviewed the form.
- **BDAU SE ISM Signature:** the signature of BDAU SE information security manager.

Once the form is complete the staff member should complete the following steps:

- Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Schema.docx.
- Save the scanned PDF to /data/master/DS001/extract/non-conformities.
- Update the BDAU SE Risk Registry using the BDAU SE Risk Registry SOP.

Version	Change
7	Updated to get signature of BDAU ISM rather than line manager as line manager ambiguous
8	Reviewed: no major changes Modified: Formatting issues

	Typo
9	Reviewed: no major changes
10	Removed: changes greater than last 5 changes
11	Fixed link to the BDAU SE Record Naming Schema, added instructions for processing forms when working remotely

BDAU SE Onboarding SOP

Document Number	75446806
DR Document Number	75446803
Content Approval	See comments for version / approver
Version Number	8
Previous Active Version Number	5
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Feb 19, 2020 15:49

This document describes the procedures for on-boarding of BDAU SE users and BDAU SE information assets.

Procedure

User Procedure

Users of the BDAU SE are expected to abide by all policies and procedures as documented under BDAU SE documentation in the Wiki. Failure to do so could result in possible removal of access, possible investigation and possible disciplinary measures.

From 01 Dec 2018 onwards both staff and users are required to complete training as per BDAU SE User Registration SOP

Staff Procedure

The on-boarding process is a 4 step process and is performed in a specific order (if an exception is required see BDAU SE Exception Registration SOP):

1. **BDAU SE User Registration SOP**
   The user registration process:
   - **DOES** associate the user with the BDAU SE
   - **DOES** grant login access to the BDAU SE
   - **DOES** require the user to follow guidelines for access to the BDAU SE
   - **DOES NOT** grant access to datasets (this is done under the dataset registration process)
   - **DOES NOT** give the user access to hold data outside the BDAU SE (this is done by exception only)
2. **BDAU SE Vendor Evaluation SOP**
   This evaluation is done if the user requires a dataset for which a vendor evaluation form does not exist. The vendor evaluation process:
   - **DOES** hold the details of the vendor contact information
   - **IS** required for a dataset evaluation
   - **DOES NOT** grant access to datasets (this is done under the dataset registration process)
   - **DOES NOT** give the user access to hold data outside the BDAU SE (this is done by exception only)
3. **BDAU SE Dataset Evaluation SOP**
   This evaluation is done if the user requires a dataset for which a dataset evaluation form does not exist. The dataset evaluation process:
   - **DOES** hold the details of a dataset including the project lead, the transfer method, the information type and the archive requirements
   - **IS** required for a dataset registration
   - **DOES NOT** grant access to datasets (this is done under the dataset registration process)
   - **DOES NOT** give the user access to hold data outside the BDAU SE (this is done by exception only)
4. **BDAU SE Dataset Registration SOP**
   This registration is done if the user requires access to a dataset. The dataset registration process:
   - **DOES** associate the user with a particular dataset
   - **DOES** grant access to a particular dataset
   - **DOES** require the project lead for the dataset is notified and approves of access
   - **DOES NOT** give the user access to hold data outside the BDAU SE (this is done by exception only)

Version	Change
4	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
5	Updated to reference new training from BDAU SE User Registration SOP
6	Reviewed: no major changes Edited Table of Contents formatting Typo
7	Reviewed: no major changes Typo
8	Reviewed: no major changes

BDAU SE Risk Registry SOP

Document Number	75451672
DR Document Number	75451669
Content Approval	See comments for version / approver
Version Number	11
Previous Active Version Number	10
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 24, 2022 13:48

This document describes how to manage risk and update and record non-conformities inside the BDAU SE Risk Registry stored under DS001.

Procedure

Staff Procedure

Staff are required to update the BDAU SE Risk Registry in "/data/master/DS001/extract/registries/Risk reg.ods" as per the BDAU SE Corrective And Preventative Action Policy. An associated BDAU SE CAPA Form.docx should exist for each non-conformity recorded (for non-major nonconformities, save email trails instead and for preventive risks no form is needed).

Please follow the Risk Management Cycle to deal with risks as they arise.

Risk Management Cycle:

1. Identify risk and determine what sort of risk it is: Business, Compliance, External, Financial and Reputational
2. Notify BDAU ISM of the risk
3. Agree what can be done to evaluate risk
4. Identify suitable response to minimize the risk
5. Implement response solution
6. Fill in risk registry using the steps below

   Fields for the BDAU SE Risk Registry are:

   - Risk Type - The risk type classifies the impact scope of the non-conformity and possible entries are listed below:
     - Business - scope of impact is on-going continuity of business as usual, risk will inhibit BDAU SE to exist or provide services.
     - Compliance - scope of impact is lack of adherence to legal, regulatory or information asset specific requirements.
     - External - scope of impact is outside of direct BDAU SE control.
     - Financial - scope of impact is loss of revenue or fines as a result of non-conformity.
     - Reputational - scope of impact is negative reputation associated with non-conformity.
   - Asset Local ID - Specific asset local ID as defined per BDAU SE Asset Registry SOP, if not tied to a specific asset or vendor mark as NA.
   - Risk Description - Long description of non-conformity and impact on BDAU SE.
   - C - Does this risk affect confidentiality of information assets (Y/N).
   - I - Does this risk affect integrity of information assets (Y/N).
   - A - Does this risk affect availability of information assets (Y/N).
   - Risk Occurrence Score - Score as 1 - 5 for occurrence of non-conformity as per below:
     - 1 - Very unlikely to occur
     - 2 - Unlikely to occur
     - 3 - Could occur or has occurred
     - 4 - Likely to occur or likely to occur again
     - 5 - Very likely to occur or very likely to reoccur
   - Risk Impact Score - Score as 1 - 5 for impact of non-conformity as per below:
     - 1 - Little to no impact
     - 2 - Minor impact (minimal or short term)
     - 3 - Moderate impact
     - 4 - Serious impact (could impact short or long-term strategy)
     - 5 - Severe impact (could require downtime of services to resolve or could halt operations completely)
   - Risk Score - Risk Occurrence Score multiplied by Risk Impact Score
     - 0 - 5 - Low risk non-conformity, should be resolved if possible
     - 6 - 9 - Medium risk non-conformity, should be resolved within the next year
     - 10 + - High risk non-conformity, should be resolved within the next 3 months
   - CAPA ID - Document ID for CAPA Form.

- SoA Annex - Annex control identifier from Statement of Applicability (SoA) which relates to this risk (top related item or section).
- Treatment Plan - High-level risk treatment plan intended to mitigate risk.
- Revised Occurrence Score - Score as 1 - 5 for occurrence of non-conformity **after** implementation of CAPA Plan, same definitions as Risk Occurrence Score.
- Revised Impact Score - Score as 1 - 5 for impact of non-conformity **after** implementation of CAPA Plan, same definitions as Risk Impact Score.
- Revised Risk Score - Revised Occurrence Score multiplied by Revised Impact Score, same definitions as Risk Score but reflects changes **after** implementation of CAPA Plan.
- Risk Owner - Email of responsible risk owner, normally bdau@imperial.ac.uk.
- Raised On - Date the non-conformity was first raised to the BDAU SE staff.
- Raised By - Email of person or group who raised the non-conformity.
- Last Reviewed On - Date the non-conformity was last reviewed by BDAU SE staff.
- Last Reviewed By - Email of person or group who last reviewed the non-conformity.
- Resolve By - Target date for resolution of the non-conformity.
- Resolved On - Date the non-conformity was actually resolved.

7.Review effectiveness through audit schedule

Note that the procedure for reporting will change once the BDAU SE has migrated to a new Quality Management System (QMS).

Version	Change
7	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12 Removed: changes greater than last 5 changes
8	Reviewed: no major changes
9	Added: Risk management cycle
10	Reviewed: no major changes
11	Updated staff procedure: exceptions for when a CAPA form is not needed, corrected typos, formatting

BDAU SE Staff Working Areas SOP

Document Number	75446337
DR Document Number	75446334
Content Approval	See comments for version / approver
Version Number	14
Previous Active Version Number	13
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Oct 28, 2021 15:46

This document describes the user and staff procedures for operating and using BDAU SE staff working areas. BDAU SE staff working areas contain sensitive documents and therefore require strict access control procedures as per below.

Procedure

User Procedure

Items below are in no particular order and must all be fully adhered to:

- Users are **NOT** allowed to access BDAU SE staff working areas without the presence of BDAU SE staff.
- Users are **NOT** allowed to share access to users who are not authorised for access by BDAU SE staff.
- Users are **ONLY** allowed to use workstations provided in BDAU SE staff areas designated for users.
- Users are **NOT** allowed to plug in their own devices into ethernet ports in BDAU SE areas without prior BDAU SE approval.
- Users will **NOT** stay logged into BDAU SE staff working area workstations without prior approval from BDAU SE staff.
- Users will **NOT** leave sensitive information on their desks.
- Users will **NOT** leave devices unlocked when not in the presence of the device.

Staff Procedure

Items below are in no particular order and must all be fully adhered to:

- Staff are **NOT** allowed to leave users unsupervised in BDAU SE staff working areas.
- Staff are **NOT** allowed to give users access to BDAU SE staff workstations.
- Staff will **NOT** allow users to plug in USB devices into BDAU SE staff workstations without prior approvals.
- Staff will **NOT** leave sensitive information on their desks.
- Staff will **NOT** leave devices unlocked when not in the presence of the device.
- Staff **WILL** store paper copies of BDAU SE registration forms within the cabinet which is locked after use.
- Staff will **NOT** hand over keys to cabinets to non-BDAU SE staff.
- Staff **WILL** use the BDAU SE Mobile to send passwords and other information to BDAU SE users.
- Staff **WILL** lock away the BDAU SE Mobile when it is not in use.

Staff Relocation Procedure

Due to unforeseen circumstances BDAU SE staff may need to relocate to another area if normal staff working areas are not available:

- This will be coordinated through communication with staff/bdau@imperial.ac.uk
- If you arrive at work and the BDAU SE staff area is not available
  - Please email bdau@imperial.ac.uk from your mobile device that the area is not available
  - If you have no further instructions yet from the BDAU SE ISM then please return to your home if safe to do so (if it is not safe to do so seek the closest emergency personnel)
- If necessary work from home using the BDAU SE Remote Working SOP
- If provided instructions for a new BDAU SE staff area from the BDAU SE ISM, please follow these instructions

When working remotely (i.e. not in the usual BDAU SE Staff Working Areas), you must follow the BDAU SE Remote Working SOP.

Version	Change
10	Removed privileged workstations and staff are not allowed to provide users of BDAU SE staff working areas with the pin code combination for doors
11	Add details regarding BDAU cabinet and phone to staff procedure
12	Fixed versions/change log
13	Reviewed: no major changes
14	Removed items related to privileged workstations and N3 connections as no longer applicable, added BDAU SE Remote Working SOP, removed the email confirmation proof for user sharing access

BDAU SE User Registration SOP

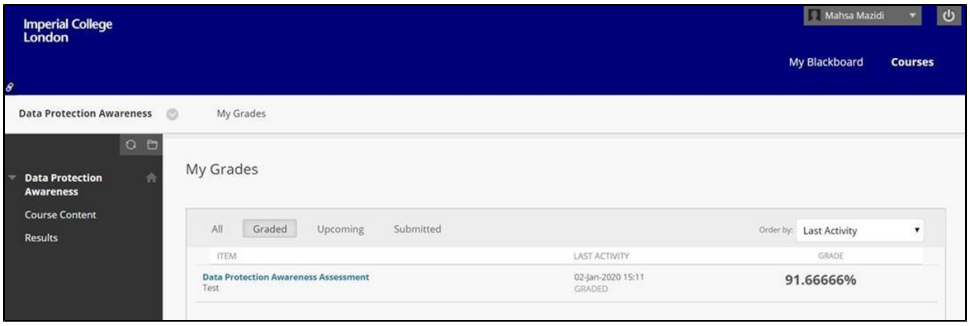
Document Number	75442531
DR Document Number	75442422
Content Approval	See comments for version / approver
Version Number	22
Previous Active Version Number	21
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 10, 2022 16:29

This document describes how to complete the BDAU SE user registration process. This is required in order to be granted an account within the BDAU Secure Environment. **Note that this does not grant access to datasets.** To be granted access to data within the BDAU Secure Environment, after completion of the BDAU SE user registration process (i.e. this SOP), the BDAU SE Dataset Registration SOP must be completed.

Procedure

User Procedure

1. **Form**
   a. The first step is to register using the BDAU SE User Registration Form.docx (click on the link to download the latest version of the form). This form covers the agreement between yourself and the BDAU in regards to appropriate use and access for the BDAU Secure Environment.
      i. If you are on an **honorary** contract with Imperial (visitors or any non-employee status are considered honorary), you will need to state:
         1. When that contract ends
         2. What your host institution is
      ii. You will need to provide a **billing contact** email
         1. If you are billing from Department of Primary Care and Public Health (PCPH), this is b.cerutti@imperial.ac.uk
         2. If you are billing under CHEPI/Business School, this will be jack.olney@imperial.ac.uk
         3. Any other users must provide the email of their **academic supervisor** or **line manager**
   b. Once this form has been completed, it can be scanned and sent to bdau@imperial.ac.uk for processing. Please note:
      i. This form is only valid until the next 31st of January
      ii. Your access will be removed automatically if you do not renew your agreement
      iii. By signing the agreement the BDAU SE user understands that they will be held liable for not following the agreement
2. **Training**
   a. Users are also required to complete GDPR Training and ISA Training and send the certificates to bdau@imperial.ac.uk, **in PDF forma**t. Please note:
      i. Certificates are required to be sent to BDAU in PDF format, no other format will be accepted. You can print to PDF or save an image and then print to PDF.
      ii. Certificate must show scores in percentages (not just pass/fail), date and time (similar to the image below). To access your training score in the format shown below:
         1. Log in to Imperial's Blackboard https://www.imperial.ac.uk/admin-services/ict/self-service/teaching-learning/blackboard/
         2. Under 'My Courses' tab, click on 'Data Protection Awareness' or 'Information Security Awareness' training
         3. From the menu bar on the left, click on 'Results' or 'My Grades' (if you do not see the menu bar, click on the grey arrow on the left)
         4. Under 'Marked'/'Graded' tab, your test result can be seen in the correct format as shown below

5. 

iii. Certificates will be checked for a passing score (70%+), but no further decisions based on score will be made

3. **Preparatory Work**
    a. Once you have sent the form and training certificates to bdau@imperial.ac.uk, complete the BDAU SE Server Access Preparatory Work SOP
    b. After you have completed the necessary preparatory work, **let us know (via Signal or official College email) that you have installed and configured Signal and Authenticator**. Additional next key instructions for connecting to the BDAU SE will then be sent to you via Signal.
4. **Server Access**
    a. Once you have received, via Signal, your BDAU SE initial TOTP token, use the BDAU SE Server Access SOP appropriate for your operating system to log into the BDAU server

Staff Procedure

1. Email user the link to BDAU SE User Registration SOP, ask them to follow the intructions as per the User Procedure
2. On receipt of the completed BDAU SE User Registration Form.docx and training certificates, the BDAU SE staff is responsible for completing the user registration process using the instructions below:
    a. Save the user's GDPR and ISA training certificates to /data/master/DS001/extract/training/users (after checking the date, format and passing score (70%+))
    b. Sign the form (note that BDAU delegates in other business lines may also sign forms)
    c. Obtain the BDAU SE ISM signature on the form
    d. Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Schema.docx.
    e. Save document from email to BDAU SE User Registrations directory (/data/master/DS001/extract/registrations/users).

    > ⚠ Make sure the document is named exactly as per the BDAU SE Record Naming Schema.docx.

    f. Complete steps in BDAU SE User Addition SOP.

Version	Change
18	Reviewed: no major changes
19	Updated User Procedure for the new BDAU SE server: Added subheadings, Aadded 1.a and 1.b, Removed 'The BDAU may not add your account without this training' as training are now compulsory, Added screenshot to step 3, Modified step 4, Added step 5 Modified: Staff Procedure for the new BDAU SE server (added setp 1, changed step 2.a, to check and save the training certificates, step 2.d, '(If forms are processed remotely, this step can be skipped)', removed step 'Configure the users initial session using their initial password' of Staff Procedure as no longer needed in the new BDAU SE
20	Updated ISA training website link
21	Added instructions for accessing the training scores
22	Fixed the link to the record naming schema, clarifications, formatting

BDAU SE User Renewal SOP

Document Number	250299978
DR Document Number	250299961
Content Approval	See comments for version / approver
Version Number	2
Previous Active Version Number	1
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 10, 2022 11:44

This document describes how to complete the BDAU SE user renewal process. All users with access to the BDAU SE must renew their registration in January of each year before their current registration expire on 31st of January. Failure to comply will result in loss of access.

Procedure

User Procedure

The renewal process requires the BDAU SE User to complete:

1. A **new User Registration form** as per the BDAU SE User Registration SOP (step 1 of the User Procedure)
   - If you do not wish to renew your registration, you must complete the user procedure in the BDAU SE User Removal SOP and notify us.
2. The **GDPR and ISA training** as per the BDAU SE User Registration SOP (step 2 of the User Procedure)
   - If you have completed your GDPR and ISA training after this December, there is no need to complete them again. Training completed at any earlier dates will need to be completed again.
3. A **new Dataset Registration form** for each dataset you are part of (if you wish to maintain access), as per the BDAU SE Dataset Registration SOP
   - If you no longer require access to any of the datasets you are part of, you must complete the BDAU SE User Removal from a Dataset SOP.
   - If the project associated with any of the datasets you are part of is completed, you must complete the user procedure in the BDAU SE Dataset Destruction and Archiving SOP.
4. Send your completed forms and training certificates to bdau@imperial.ac.uk, all in one email, **before 31st of January**.

Staff Procedure

- Generate a list of current BDAU SE users and their associated datasets by running the following commands:

  To generate a list of the current and valid secure gateway usernames

  ```
  /opt/bdau/server/bin/DLsgmembers.py
  ```

  To generate a list to show which usernames relate to which datasets

  ```
  /opt/bdau/server/bin/DLmembership.py all
  ```

- Send out the User Renewal email in December (using template below) along with the excel spreadsheet generated in the previous step:
  - **Email title: “Compliance - BDAU SE User Renewal XXXX” (where xxxx is the next year, e.g. 2021)**
  - **Make sure to attach the excel spreadsheet to the email**
  - **Replace XXXX in the template below with the next year e.g. 2021**

Compliance - BDAU SE User Renewal XXXX
Dear BDAU SE Users,

It is time to renew all training and user and dataset registration forms for XXXX, as your current registration will expire on 31st of January. Please follow the renewal instructions carefully from the BDAU SE User Renewal SOP (https://wiki.imperial.ac.uk/display/MB/BDAU+SE+User+Renewal+SOP - College login is required). Failure to comply will result in **loss of access**.

Please make sure to use the latest version of the forms which are available to download from the link provided.

You will find attached the list of datasets that you are a member of. If you no longer require access to your dataset(s) and/or to the BDAU SE, please complete the BDAU SE User Removal from a Dataset SOP and/or the BDAU SE User Removal SOP and let us know by replying to bdau@imperial.ac.uk.

Regarding the data contained in the attached spreadsheet, this is public domain as all data comes from the College LDAP system and is accessible by any user with a College account.

At BDAU, we keep your personal data confidential and only use it as part of our operational work, maintaining a copy in both digital and physical format and will keep it for a minimum of 10 years. We operate under the privacy notice for staff of Imperial College. The only information which is not internally available would be your phone number and CID. As stated, these will be used only to provide our service to you including auditing when required. Please see https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/ICL---Privacy-Notice-for-Staff-and-Prospective-Staff-March-2019.pdf for more information.

As you know, BDAU user fees are billed on a per user per year basis. We will be in touch regarding this where applicable in the new year.

Please let us know if you have any other questions.

Best wishes

BDAU Team

- Send out reminder emails (e.g. one in mid-January and one final reminder in the last week of January)
- On receipt of the user's completed forms and training certificates, the BDAU SE staff are responsible for completing the user renewal process using the instructions below:
    1. GDPR and ISA training certificates:
        a. Check the date, passing score (70%+) and format of the certificates. Ask user to re-do if the certificates do not meet the criteria specified in the BDAU SE User Registration SOP.
        b. Save the user's training certificates to `/data/master/DS001/extract/training/users`, with documents named as per BDAU SE Record Naming Schema.docx
    2. User Registration and Dataset Registration forms:
        a. Review and sign the form (note that BDAU delegates in other business lines may also sign forms).
        b. Obtain the BDAU SE ISM signature on the form.
        c. Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Schema.docx
        d. Save document from email to BDAU SE User or Dataset Registrations directories (under `/data/master/DS001/extract/registrations/`).

        > ⚠ Make sure the document is named exactly as per BDAU SE Record Naming Schema.docx

- Follow up with non-compliant users in February to ensure they have completed the BDAU SE User Removal SOP.
- Remove the non-compliant users from the BDAU SE as per the BDAU SE User Removal SOP.

Version	Change
1	Document creation Added DR Document Number Added published Document Number
2	Added Linux command steps to Staff Procedure

BDAU SE Vendor Evaluation SOP

Document Number	75442504
DR Document Number	75442407
Content Approval	See comments for version / approver
Version Number	8
Previous Active Version Number	7
Review Cycle (months)	12
Document Type	Procedure
Last Modified Date	Mar 10, 2022 16:12

This document describes how to complete the BDAU SE Vendor Evaluation process for new or existing vendors. This is required in order to evaluate new datasets using the BDAU SE Dataset Evaluation SOP.

Procedure

User Procedure

1. If you wish to use a new/existing vendor within the BDAU SE environment (i.e. for a new BDAU SE Dataset), you need to work with the BDAU to complete the BDAU SE Vendor Evaluation Process.

Staff Procedure

1. Fill out the BDAU SE Vendor Evaluation Form.docx :
    a. **Vendor ID:** Next sequential vendor ID (see /data/master/DS001/extract/evaluations/vendors/*.pdf)
    b. **Vendor Name:** Name of vendor (i.e. NHS Digital)
    c. **Vendor Address:** Address of vendor
    d. **Vendor Phone Number:** Phone number of general enquiries for vendor
    e. **Vendor Email:** Email of general enquiries for vendor
    f. **Vendor Country:** Country of where vendor is based
    g. **BDAU Reviewer:** BDAU staff member performing review (email address)
    h. **BDAU Contact:** Contact to email before expiration (email address)
    i. **Valid From:** First date of valid data/software
    j. **Last Reviewed:** Date when reviewed by BDAU staff member
    k. **Requires Exception:** YES if requires exception to be used outside the BDAU SE
    l. **User Restricted:** YES if restricted to particular users
    m. **Retention Period:** How long is the vendor data retained for
    n. **Archived:** YES if no longer in use
2. Once form has been completed, print out and sign
    a. **BDAU SE Authorisation:** BDAU staff member signature, printed name and signing date
    b. **BDAU SE ISM Authorisation:** BDAU ISM signature, and printed name and signing date
3. Scan document and email to bdau@imperial.ac.uk (when working remotely, email the processed form to bdau@imperial.ac.uk) with subject as name of document as per BDAU SE Record Naming Scheme.rtf
4. Save document from email to BDAU SE Vendor Evaluations directory (/data/master/DS001/extract/evaluations/vendors)
5. Add to BDAU SE Asset Registry with appropriate fields as per the BDAU SE Asset Registry SOP

Version	Change
4	Updated last active version Updated saving instructions
5	Reviewed: no major changes Added: last modified Modified: review cycle 6 to 12

	Removed: changes greater than last 5 changes
6	Removed: Risk score, Valid To Added: Vendor Country, Retention Period
7	Reviewed: no major changes Modified: Wording in Step 2b
8	Added: a link to the vendor evaluation form, signing date for authorisation, processing forms when working remotely