**DART RBC OFFLINE FORM – INFORMATION**

On completion, either E-Mail the form to our MODNet S mailbox (ISSDes-DAIS-RBC@modnet.s.mil.uk) or double envelope and dispatch using Parcelforce with end-to-end ‘Track and Trace’ as well as both notification & receipt of delivery (e.g. Parcelforce Express24) to:

Service Delivery Team, CyDR, Room X007,

Bazalgette Pavillion, RAF Wyton,

Huntingdon, Cambs, PE28 2EA

**For all enquiries email:** UKStratComDD-CyDR-DART-Help@mod.gov.uk (information supplied to be no higher than OFFICIAL SENSITIVE (OS))

THIS FORM IS TO BE USED WHEN THE INFORMATION BEING ENTERED IS LIKELY TO BE CLASSIFIED SECRET **AND/OR** THE INFORMATION ABOUT WHICH THE RBC IS BEING RAISED IS DEEMED TO BE SECRET OR ABOVE. IN ALL OTHER INSTANCES, PLEASE USE THE OFFICIAL SENSITIVE (OS) VERSION OF THIS FORM.

|  |
| --- |
| Any question within a red box is **MANDATORY** and **MUST** be filled in for the submission to be accepted. |

|  |
| --- |
| Please note that this document should be treated as **SECRET** when completed |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RBC REGISTRATION** | | | | | |
| R0010.1 | Please state the name of the System/Application/Platform to which this RBC relates. |  | | | This is the name that will appear on the dashboard. |
| R0010.2 | Please provide a brief summary of the reason for this RBC. |  | | | Please give a brief summary of why this RBC is being raised. More detailed questions will be asked further in the questionnaire - Example - Named organisation have a requirement to move an unencrypted removable SECRET Hard Drive between 3 sites (1  organisation site and 2 MOD (Abbey  Wood and RAF Wyton) for trials activities. |
| R0020.1 | Is this RBC for the movement of portable CIS or magnetic/optical media where the required encryption standards cannot be met? | Yes - Movement RBC  **(Please complete the Movement RBC Form)** | |  | Fast Track and Supplement 12 are legacy terms for different types of RBC. Fast Track RBCs are now termed Movement RBCs and are for Portable CIS (mainly laptops and hand held devices), and the transportation of magnetic/optical media where the required encryption standards cannot be met. Supplement 12 RBCs are now called Information RBCs and are for everything else |
| No - Information RBC | |  |
| R0021.1 | What is the date by which a MOD Senior Information Risk Owner (SIRO) decision is required? |  | | | DD/MM/YYYY |
| R0021.2 | Please explain why this date has been stated. |  | | | What are the key decision points; what is likely to be the effect if they are missed? |
| R0030.1 | What is the maximum Security Classification/Marking of the content of this RBC? | Official |  | | This refers to the classification of the information you will be entering on DART and not the classification of the System/TOA, or the data it holds/processes. I.E. if you wrote this RBC on a paper form, what classification would the document be? |
| Official Sensitive |  | |
| Secret or Above |  | |
| **IF ANSWER TO R0030.1 WAS “SECRET OR ABOVE” DO NOT CONTINUE THIS FROM. PLEASE PROCEED TO THE APPROPRIATE DOMAIN** | | | | | |
| R0040.1 | Has the System/Application/Platform to which this RBC relates, been registered on DART (Defence Assurance Risk Tool) for accreditation? | Yes | | | Please annotate the desired row  All systems and applications processing MOD data require accreditation, DART is used to record this. |
| No | | |
| Not Known | | |
| **ONLY ANSWER THE NEXT QUESTION IF ANSWER TO R0040.1 WAS “DART”** | | | | | |
| R0050.1 | Please enter details of the Target(s) of Assurance to which this RBC relates or the DART ID(s). | . | | | Where the RBC relates to more than one DART ID, please list them all. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R0060.1 | Which Top Level Budget (TLB)/Enabling Organisation (EO) is responsible for this RBC? | Navy Command | | | |  | Please annotate the desired row.  The TLB/EO responsible for the system/platform that this RBC is being raised against. |
| Army Headquarters | | | |  |
| Air Command | | | |  |
| Air (Space Command) | | | |  |
| UK Strategic Command (UKStratCom) | | | |  |
| Defence Business Services (DBS) | | | |  |
| Defence Equipment & Support (DE&S) | | | |  |
| DE&S LogIS/BTG | | | |  |
| Defence Nuclear Organisation (DNO) | | | |  |
| Defence Infrastructure Organisation (DIO) | | | |  |
| MOD Head Office | | | |  |
| Defence Science & Technology Laboratory (DSTL) | | | |  |
| UK Hydrographic Office (UKHO) | | | |  |
| MOD Police (MDP) | | | |  |
| Defence Electronics and Components Agency (DECA) | | | |  |
| Other (Please provide details in adjacent box) | | | |  |  |
| **ONLY ANSWER THE NEXT QUESTION IF ANSWER TO R0060.1 WAS “UK STRATEGIC COMMAND (UKStratCom)”** | | | | | | | |
| R0065.1 | Within UKStratCom, who is the lead HLB responsible for this RBC? | PJHQ (Permanent Joint Headquarters) | | | |  | Who holds the Risk? Generally speaking, this would be the HLB who would be most impacted should the risk be realised. |
| Special Military Units (SMU) | | | |  |
| Joint Force Development and Defence Academy | | | |  |
| DI (Defence Intelligence) | | | |  |
| DD (Defence Digital) | | | |  |
| Surgeon General | | | |  |
| Assistant Chief of the Defence Staff (Logistics) | | | |  |
| Joint Force Development and Defence Academy | | | |  |
| Joint Commands such as the Permanent Joint Operating Bases (PJOBs) and Joint Counter Terrorism Training and Advisory Team and Joint Arms Control Implementation Team | | | |  |
| Other (Please provide details in adjacent box) | | | |  |  |
| **CONTINUE FORM AS NORMAL**  **RBC OUTLINE** | | | | | | | |
| R0110.1 | Please provide any alternative reference for this RBC, if required. | Reference |  | | | Please note that the RBC ID allocated when the information is uploaded into DART, will be the principal ID used. However alternative references might include your own internal reference number, or that of the FLC/MBU, or a relevant risk register reference. Please indicate the type of reference as well as the reference number itself. | |
| Type of the Reference |  | | |
| R0120.1 | Which of the following best describes the category of RBC. Please tick all that apply. | Cryptography (CRYPTO) | | |  | Please tick all that apply. The categories are defined as:  Crypto - RBCs dealing with risks related to cryptographic products. E.g. use beyond stated LYOU.  TEMPEST - RBCs dealing with tempest issues. E.g. where operational imperatives prevent compliance with testing regimes.  Portable CIS - RBCs dealing with mainly laptops where no, or insufficient, encryption is present. Infrastructure - RBCs relating to physical infrastructure/components. E.g. an unencrypted cable run in a coalition environment carrying UKEO data.  Personal Data - RBCs where personal data is involved.  Media Encryption - RBCs dealing with the encryption & movement of CDs/DVDs/HDDs/USB sticks etc where encryption does not meet the required standard, or is absent.  Data in transit - RBCs dealing with the electronic movement of data. E.g breaking/not breaking HTTPS sessions. Data at Rest - RBCs dealing with the storage of data. E.g. IL5 data stored on an IL3 system. Foreign Nationals - RBCs dealing with FNs (typically allies) access to information. Obsolete SW/Patching/AV - RBCs dealing with out of date SW, lack of SW patching or lack of AV protection. E.g. Use of Windows XP beyond end of support. | |
| TEMPEST | | |  |
| Portable Communications & Information Systems (CIS) | | |  |
| Infrastructure | | |  |
| Personal Data | | |  |
| Media Encryption | | |  |
| Data in Transit | | |  |
| Data at Rest | | |  |
| Foreign Nationals | | |  |
| Obsolete Hardware (H/W), Software (S/W) or lack of Anti-Virus Protection | | |  |
| Other (Please provide details in adjacent box) | | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0120.1 WAS “Personal Data”** | | | | | | | |
| R0123.1 | Please provide the number of personal records being processed and provide a brief description. | Quantity | |  | |  | |
| Description | |  | |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R0123.2 | Whose personal data is at risk? Please tick all that apply. | General Public | | | |  |  |
| MOD Civilian (Including embedded contractors) | | | |  |  |
| British Forces Personnel | | | |  |  |
| Foreign Military Forces personnel | | | |  |  |
| Other (Please provide details in adjacent box) | | | |  |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0120.1 WAS “Foreign Nationals”** | | | | | | | |
| R0121.1 | What level of Defence Network (MODNet) access do foreign nationals need? | None |  | | |  | |
| MODNet OFFICIAL |  | | |
| MODNet SECRET |  | | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0121.1 WAS “MODNet SECRET”** | | | | | | | |
| R0122.1 | Please provide details for access to Defence Networks. | Name of Person | |  | |  | |
| PUID | |  | |
| Tour Expiry/Expiration (TOUREX) | |  | | DD/MM/YYYY | |
| **CONTINUE FORM AS NORMAL** | | | | | | | |
| R0130.1 | Does this RBC relate to an Urgent Operational Requirement (UOR)? | Yes | | |  |  | |
| No | | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0130.1 WAS “YES”** | | | | | | | |
| R0131.1 | Please provide a justification as to why this is a UOR. |  | | | | You must provide some details of the Op, including reasons for the urgency. | |
| **CONTINUE FORM AS NORMAL** | | | | | | | |
| R0140.1 | Describe, in layman's terms, the issue(s) that have necessitated the raising of this RBC? |  | | | | This is characterised by a conflict between security advice and business need that requires resolution, for example:   * **Security Viewpoint**: the residual information security risk is unacceptable; * **Business viewpoint**: the proposed capability is needed strongly enough that the residual risk should be accepted. | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R0140.2 | Describe, in layman's terms, the Business Requirement that this RBC is intended to meet. | |  | | | | | | |  |
| **DATA** | | | | | | | | | | |
| R0150.1 | What is the maximum Security Classification of the information handled? | | Official | | |  | | | |  |
| Official Sensitive | | |  | | | |
| Secret | | |  | | | |
| North Atlantic Treaty Organisation (NATO) Secret | | |  | | | |
| Top Secret | | |  | | | |
| North Atlantic Treaty Organisation (NATO) Top Secret | | |  | | | |
| R0160.1 | What Descriptors (if any) apply to the information handled? Please tick all that apply or 'None'. | | Personal | | | | |  | |  |
| Commercial | | | | |  | |
| Location Sensitive (LOCSEN) | | | | |  | |
| Limited Circulation | | | | |  | |
| Other | | | | |  | |
| None | | | | |  | |
| R0170.1 | What Caveats are applied to the information handled? Please tick all that apply. | | AUS/NZ/UK/US only | | | | |  | |  |
| AUS/CAN/NZ/UK only | | | | |  | |
| AUS/CAN/NZ/UK/USonly | | | | |  | |
| AUS/CAN/UK/US only | | | | |  | |
| AUS/UK/US only | | | | |  | |
| CAN/UK/US only | | | | |  | |
| CAN/AUS/UK/US/Ger/Dnk/Fr/It only | | | | |  | |
| AUS/UK only | | | | |  | |
| UK Eyes Discretion | | | | |  | |
| UK Eyes only | | | | |  | |
| UK/US Eyes only | | | | |  | |
| UK/US/Israel Eyes only | | | | |  | |
| Special Intelligence | | | | |  | |
| Multi-National Force (MNF-1) | | | | |  | |
| International Security Assistance Force (ISAF) | | | | |  | |
| Other (Please provide details in adjacent box) | | | | |  | |  |
| None | | | | |  | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0150.1 WAS “SECRET” OR ABOVE** | | | | | | | | | | |
| R0180.1 | | Will the information include the use of Codewords and/or Compartment Categories? | | Yes | | | |  | |  |
| No | | | |  | |
| **CONTINUE FORM AS NORMAL** | | | | | | | | | | |
| R0190.1 | What is the information at risk? | |  | | | | | | | Please provide a brief summary of what the information at risk is - Example: The information at risk is the personal data records for service personnel within this establishment. It covers their clearance details, previous work history and medical details. |
| **ASSETS** | | | | | | | | | | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0120.1 WAS “PORTABLE COMMUNICATION & INFORMATION SYSTEMS (CIS)” OR “MEDIA ENCRYPTION”** | | | | | | | | | | |
| R0490.1 | Please indicate which types of assets are covered by this RBC. Please annotate all that apply. | | Laptops | | | |  | |  | |
| Compact Disk(CD)/Digital Video Discs(DVDs) | | | |  | |
| Memory Cards | | | |  | |
| Universal Serial Bus(USB) Drives | | | |  | |
| Tablets | | | |  | |
| Personal Digital Assistants(PDAs) | | | |  | |
| Smart Phones/Portable Messaging Devices(PMD) | | | |  | |
| External Hard Drives | | | |  | |
| Tape Drives | | | |  | |
| Other (Please provide details in adjacent box) | | | |  | |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “LAPTOPS”** | | | | | | | | | | |
| R0500.1 | Please indicate the total number of laptop assets involved and provide the serial numbers of these assets. | | Laptop Quantity | |  | | | | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. | |
| Laptop Serial Number/s | |  | | | |
| R0500.2 | Are the assets encrypted? | | Yes | |  | | | |  | |
| No | |  | | | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0500.2 WAS “YES”** | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R0501.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  |
| R0501.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  |  |
| Enhanced |  |
| Baseline |  |
| Commercial |  |
| R0501.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  |  |
| Partial |  |
| None |  |
| R0502.1 | Are you complying fully with encryption policy? | Yes |  |  |
| No |  |
| Not Applicable |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0502.1 WAS “NO”** | | | | |
| R0503.1 | Please explain the reason for non-compliance with encryption policy. |  | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “COMPACT DISK(CD)/DIGITAL VIDEO DISCS(DVDS)”** | | | | |
| R0510.1 | Please indicate the total number of Compact Disk (CD)/Digital Video Discs (DVD) assets involved and provide the serial numbers of these assets. | CD/DVD Quantity |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| CD/DVD Serial Number/s |  |
| R0510.2 | Are the assets encrypted? | Yes |  |  |
| No |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0510.2 WAS “YES”** | | | | |
| R0511.1 | Please state the product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  |
| R0511.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  |  |
| Enhanced |  |
| Baseline |  |
| Commercial |  |
| R0511.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  |  |
| Partial |  |
| None |  |
| R0512.1 | Are you complying fully with encryption policy? | Yes |  |  |
| No |  |
| Not Applicable |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0512.1 WAS “NO”** | | | | |
| R0503.1 | Please explain the reason for non-compliance with encryption policy. |  | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “MEMORY CARDS”** | | | | |
| R0520.1 | Please indicate the total number of Memory Card assets involved and provide the serial numbers of these assets. | Memory Card Quantity |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| Memory Card Serial Number/s |  |
| R0520.2 | Are the assets encrypted? | Yes |  |  |
| No |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0520.2 WAS “YES”** | | | | |
| R0521.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  |
| R0521.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  |  |
| Enhanced |  |
| Baseline |  |
| Commercial |  |
| R0521.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  |  |
| Partial |  |
| None |  |
| R0522.1 | Are you complying fully with encryption policy? | Yes |  |  |
| No |  |
| Not Applicable |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0522.1 WAS “NO”** | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R0523.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “UNIVERSAL SERIAL BUS (USB) DRIVES”** | | | | | |
| R0530.1 | Please indicate the total number of Universal Serial Bus (USB) Drive assets involved and provide the serial numbers of these assets. | USB Drive Quantity | |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| USB Drive Serial Number/s | |  |
| R0530.2 | Are the assets encrypted? | Yes | |  |  |
| No | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0530.2 WAS “YES”** | | | | | |
| R0531.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name | |  | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard | |  |
| R0531.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High | |  |  |
| Enhanced | |  |
| Baseline | |  |
| Commercial | |  |
| R0531.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full | |  |  |
| Partial | |  |
| None | |  |
| R0532.1 | Are you complying fully with encryption policy? | Yes | |  |  |
| No | |  |
| Not Applicable | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0532.1 WAS “NO”** | | | | | |
| R0533.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “TABLETS”** | | | | | |
| R0540.1 | Please indicate the total number of Tablet assets involved and provide the serial numbers of these assets. | Tablet Quantity | |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| Tablet Serial Number/s | |  |
| R0540.2 | Are the assets encrypted? | Yes | |  |  |
| No | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0540.2 WAS “YES”** | | | | | |
| R0541.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name | |  | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard | |  |
| R0541.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High | |  |  |
| Enhanced | |  |
| Baseline | |  |
| Commercial | |  |
| R0541.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full | |  |  |
| Partial | |  |
| None | |  |
| R0542.1 | Are you complying fully with encryption policy? | Yes | |  |  |
| No | |  |
| Not Applicable | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0542.1 WAS “NO”** | | | | | |
| R0543.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “PERSONAL DIGITAL ASSISTANTS (PDAs)”** | | | | | |
| R0550.1 | Please indicate the total number of Personal Digital Assistant(PDA) assets involved and provide the serial numbers of these assets. | PDA Quantity | |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| PDA Serial Number/s | |  |
| R0550.2 | Are the assets encrypted? | Yes | |  |  |
| No | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0550.2 WAS “YES”** | | | | | |
| R0551.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R0551.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  | |  |
| Enhanced |  | |
| Baseline |  | |
| Commercial |  | |
| R0551.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  | |  |
| Partial |  | |
| None |  | |
| R0552.1 | Are you complying fully with encryption policy? | Yes |  | |  |
| No |  | |
| Not Applicable |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0542.1 WAS “NO”** | | | | | |
| R0553.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “SMART PHONES/PORTABLE MESSAGING DEVICES(PMD)”** | | | | | |
| R0560.1 | Please indicate the total number of Smart Phone/Portable Messaging Device (PMD) assets involved and provide the serial numbers of these assets. | Smart Phone/PMD Quantity |  | | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| Smart Phone/PMD Serial Number/s |  | |
| R0560.2 | Are the assets encrypted? | Yes |  | |  |
| No |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0560.2 WAS “YES”** | | | | | |
| R0561.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  | |
| R0561.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  | |  |
| Enhanced |  | |
| Baseline |  | |
| Commercial |  | |
| R0561.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full | |  |  |
| Partial | |  |
| None | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R0562.1 | Are you complying fully with encryption policy? | Yes |  | |  |
| No |  | |
| Not Applicable |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0562.1 WAS “NO”** | | | | | |
| R0563.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “EXTERNAL HARD DRIVES”** | | | | | |
| R0570.1 | Please indicate the total number of External Hard Disk Drive (HDD) assets involved and provide the serial numbers of these assets. | HDD Quantity |  | | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| HDD Serial Number/s |  | |
| R0570.2 | Are the assets encrypted? | Yes |  | |  |
| No |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0570.2 WAS “YES”** | | | | | |
| R0571.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | | Product names include: BitLocker, BeCrypt, ECLYPT, Flagstone, Lumension, WinZip, 7Zip; Standards include: Federal Information Processing Standard (FIPS) 140.2, Commercial Product Assurance (CPA), CESG Assisted Product Scheme (CAPS). |
| Asset encryption product standard |  | |
| R0571.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  | |  |
| Enhanced |  | |
| Baseline |  | |
| Commercial |  | |
| R0571.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  | |  |
| Partial |  | |
| None |  | |
| R0572.1 | Are you complying fully with encryption policy? | Yes |  | |  |
| No |  | |
| Not Applicable |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0572.1 WAS “NO”** | | | | | |
| R0573.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “TAPE DRIVES”** | | | | | |
| R0580.1 | Please indicate the total number of Tape Drive assets involved and provide the serial numbers of these assets. | Tape Driver Quantity |  | | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| Tape Drive Serial Number/s |  | |
| R0580.2 | Are the assets encrypted? | Yes |  | |  |
| No |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0580.2 WAS “YES”** | | | | | |
| R0581.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name |  | |  |
| Asset encryption product standard |  | |
| R0581.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High |  | |  |
| Enhanced |  | |
| Baseline |  | |
| Commercial |  | |
| R0581.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full |  | |  |
| Partial |  | |
| None |  | |
| R0582.1 | Are you complying fully with encryption policy? | Yes |  | |  |
| No |  | |
| Not Applicable |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0582.1 WAS “NO”** | | | | | |
| R0583.1 | Please explain the reason for non-compliance with encryption policy. |  | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0490.1 WAS “OTHER”** | | | | | |
| R0590.1 | Please indicate the total number of other assets involved and provide the serial numbers of these assets. | Other (Please describe, including quantities) | |  | Please upload a file of serial numbers if there are a large number of assets.  Please attach any files needed. |
| Other Serial Number/s | |  |
| R0590.2 | Are the assets encrypted? | Yes | |  |  |
| No | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0590.2 WAS “YES”** | | | | | |
| R0591.1 | Please state product name and/or the standard to which the encryption conforms. | Asset encryption product name | |  |  |
| Asset encryption product standard | |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R0591.2 | What grade of encryption is in use on the affected assets? Please tick all that apply. | High | | |  |  | |
| Enhanced | | |  |
| Baseline | | |  |
| Commercial | | |  |
| R0591.3 | What is the encryption status of the affected assets? Please tick all that apply. | Full | | |  |  | |
| Partial | | |  |
| None | | |  |
| R0592.1 | Are you complying fully with encryption policy? | Yes | | |  |  | |
| No | | |  |
| Not Applicable | | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0582.1 WAS “NO”** | | | | | | | |
| R0593.1 | Please explain the reason for non-compliance with encryption policy. |  | | | | If it is not possible to encrypt, explain why this is the case.  If it is possible to employ encryption, including non-compliant encryption, and this has not been done, an explanation should be given. | |
| **CONTINUE FORM AS NORMAL**  **COMPLIANCE AND POLICY** | | | | | | | |
| R0600.1 | Please provide a security impact statement. |  | | | | | This is the impact should the worst happen and a compromise were to actually occur. It is required in all cases, regardless of how unlikely it is to happen. |
| R0600.2 | Please list any existing security controls that are currently in place. |  | | | | |  |
| R0600.3 | Please provide details of any additional proposed security controls that will be put in place and the dates on which they will be implemented. |  | | | | |  |
| R0610.1 | Please indicate the applicable security policies.  (Please add the reference into the adjacent suitable box.) | JSP – Joint Services Publication | |  | | |  |
| DIAN – Defence Information Assurance Notice | |  | | |  |
| DIN – Defence Instruction and Notice | |  | | |  |
| List X Notice | |  | | |  |
| ISN – Industry Security Notice | |  | | |  |
| Other (Please provide details in adjacent box) | |  | | |  |
| R0610.2 | Please provide an explanation as to why the security policy is not being adhered to. |  | | | | |  |
| R0611.1 | Is there an action plan in place to attain policy compliance? | Yes |  | | | |  |
| No |  | | | |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0611.1 WAS “YES”** | | | | | | | |
| R0610.3 | When do you expect policy compliance to be met? |  | | | | | DD/MM/YYYY |
| R0610.5 | Please describe the action plan to attain policy compliance. |  | | | | | This refers to plans to permanently remove the non-compliance with policy. Provide the plan, with timeline, to attain compliance. |
| **CONTINUE FORM AS NORMAL** | | | | | | | |
| R0610.6 | Please describe the interim Courses of Action (CoA) proposed to mitigate the policy compliance gap. |  | | | | | This refers to any interim actions which will be implemented in order to reduce the risk in the shorter term.  Please describe the options that are available for consideration by the Top Level Budget (TLB) and MOD Senior Information Risk Owner (SIROS). Each option should include a statement of what would be done to mitigate risks in addition to the measures already in place, an action timeline, estimated costs and an assessment of the residual risk before and after the CoA is applied.  Normally there will be at least 3 options (including the 'Do Nothing' option); however, more than 3 options may be provided. |
| R0610.7 | Please describe the Course of Action (CoA) that is associated with the risk that MOD SIRO is being requested to accept. |  | | | | | Where there are multiple Courses of Action, it should be made clear which CoA, and therefore which risks, MOD Senior Information Risk Owner (SIRO) is being asked to accept. |
| R0620.1 | Do you have any relevant supporting documentation to upload? | Yes |  | | | |  |
| No |  | | | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0620.1 WAS “YES”** | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R6021.1 | Please upload the appropriate documentation, where available. | | Please attach any documents on reply and note down the document name here: | | | | Here are examples of the type of documentation you may wish to upload if applicable:   * Movement Plan * Privacy Impact Assessment (PIA) * System Diagram * Technical Case * Other evidence (Business Case/ Security) * Risk Management Accreditation Document Set (RMADS) * Security Operating Procedures (SyOps) * Security Instructions (SyIs) |
| **CONTINUE FORM AS NORMAL**  **PROJECT INFORMATION** | | | | | | | |
| R0630.1 | Does the progression of this RBC involve any key milestones or decision points? | | Yes | |  | |  |
| No | |  | |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0630.1 WAS “YES”** | | | | | | | |
| R0640.1 | Annotate the milestone dates and a brief description of the decisions that need to be made on each one of these dates. | |  | | | | DD/MM/YYYY  Decisions required at milestone point 1 |
|  | | | | | | | |
| **CONTINUE FORM AS NORMAL**  **IMPACT** | | | | | | | |
| R0650.1 | | Please indicate the **Confidentiality** Impact **prior to** mitigation and provide an explanation for this assessment. | | Red | |  |  |
| Amber | |  |
| Yellow | |  |
| Green | |  |
| R0650,2 | | Confidentiality Impact explanation. | |  | | |  |
| R0651.1 | | Please indicate the **Availability** Impact **prior to** mitigation and provide an explanation for this assessment. | | Red | |  |  |
| Amber | |  |
| Yellow | |  |
| Green | |  |
| R0651,2 | | Availability Impact explanation. | |  | | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R0652.1 | Please indicate the **Integrity** Impact **prior to** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0652,2 | Integrity Impact explanation. |  | |  |
| R0653.1 | Please indicate the **Business** Impact **prior to**, mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0653,2 | Business Impact explanation. |  | |  |
| R0654.1 | Please indicate the **Reputational** Impact **prior to** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0654,2 | Reputational Impact explanation. |  | |  |
| R0660.1 | Please indicate the **Confidentiality** Impact **post** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0660,2 | Confidentiality Impact explanation. |  | |  |
| R0661.1 | Please indicate the **Availability** Impact **post** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0661,2 | Availability Impact explanation. |  | |  |
| R0662.1 | Please indicate the **Integrity** Impact **post** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0662,2 | Integrity Impact explanation. |  | |  |
| R0663.1 | Please indicate the **Business** Impact **post** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0663,2 | Business Impact explanation. |  | |  |
| R0664.1 | Please indicate the **Reputational** Impact **post** mitigation and provide an explanation for this assessment. | Red |  |  |
| Amber |  |
| Yellow |  |
| Green |  |
| R0664,2 | Reputational Impact explanation. |  | |  |
| R0670.1 | Please describe the residual risk that will exist post mitigation. |  | |  |
| R0680.2 | Have any threat assessments been conducted? | Yes |  |  |
| No |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0680.2 WAS “YES”** | | | | |
| R0681.1 | Please provide threat assessment details. |  | | Identify relevant and applicable threat actors and their means of attack. This should include an assessment of how easy or difficult (likely) it would be for a threat to exploit the identified vulnerabilities.  Also indicate the origin/author of the threat assessment. |
| R0681.2 | Do you have another threat assessment? | Yes |  | If yes please add information alongside previous. |
| No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTINUE FORM AS NORMAL**  **OWNERSHIP** | | | | |
| R0700.1 | Which organisation(s) is/are the MOD Data Owner(s) associated with this RBC? Please tick all that apply. | Navy Command |  |  |
| Army Headquarters |  |
| Air Command |  |
| Air (Space Command) |  |
| UK Strategic Command (UKStratCom) |  |
| Defence Business Services (DBS) |  |
| Defence Equipment & Support (DE&S) |  |
| DE&S LogIS/BTG |  |
| Defence Nuclear Organisation (DNO) |  |
| Defence Infrastructure Organisation (DIO) |  |
| MOD Head Office |  |
| Defence Science & Technical Laboratory (DSTL) |  |
| MOD Police (MDP) |  |
| Defence Electronics and Components Agency (DECA) |  |
| Special Military Units (SMU) |  |
| Other (Please provide details in adjacent box) |  |
| R0700.2 | Is any of the information associated with this RBC owned by any Other Government Department (OGD)? | Yes |  | In the case of externally owned information, it will be necessary to identify two or more Risk Owners:- MOD Risk Owner: that party who would own the risk were the information entirely MOD originated; - External Information Owner(s) (EIO(s)): these should be identified. |
| No |  |
| R0700.3 | Is any of the information associated with this RBC owned by a non-UK Government or industry organisation? | Yes |  | Identify the External Information Owner(s) (EIO(s)). In these cases, the MOD Risk Owner is not empowered to make a risk balance exception decision as he does not own all of the information assets to be protected and therefore will need to engage with the EIOs. |
| No |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0700.2 WAS “YES”** | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R0710.1 | Which Other Government Departments (OGDs) own some of the information associated with this RBC? Please tick all that apply. | Attorney General's Office | | |  | |  |
| Cabinet Office | | |  | |
| Department for Business, Innovation & Skills | | |  | |
| Department for Communities & Local Govt. | | |  | |
| Department for Culture, Media & Sport | | |  | |
| Department for Education | | |  | |
| Department for Environment, Food & Rural Affairs | | |  | |
| Department for International Development | | |  | |
| Department for Transport | | |  | |
| Department for Work & Pensions | | |  | |
| Department for Energy & Climate Change | | |  | |
| Department for Health | | |  | |
| Foreign & Commonwealth Office | | |  | |
| HM Treasury | | |  | |
| Home Office | | |  | |
| Ministry of Justice | | |  | |
| Northern Ireland Office | | |  | |
| Office of the Advocate General for Scotland | | |  | |
| Scotland Office | | |  | |
| UK Export Finance | | |  | |
| Wales Office | | |  | |
| Other (Please provide details in adjacent box) | | |  |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0700.3 WAS “YES”** | | | | | | |
| R0720.1 | Which non-UK Government or industry owns some of the information associated with this RBC? Please list them in the text box provided. |  | |  | | |
| **CONTINUE FORM AS NORMAL** | | | | | | |
| R0730.1 | Have any accreditors (Cyber Defence and Risk (CyDR), Top Level Budget (TLB) or Other Government Department (OGD) already been involved in the formulation of this RBC? | Yes |  |  | | |
| No |  |
| Unknown |  |
| **ONLY ANSWER THE NEXT QUESTIONS IF ANSWER TO R0730.1 WAS “YES”** | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R0740.1 | Please provide details of the Accreditors with whom you have already been in contact. | Cyber Defence and Risk (CyDR) Accreditor 1 |  | Supply the Rank/Title, Name, Phone Number and Email Address of each accreditor. This should be accreditor for the information system this RBC is being raised against. | |
| Cyber Defence and Risk (CyDR) Accreditor 2 |  |
| Top Level Budget (TLB) Accreditor 1 |  |
| Top Level Budget (TLB) Accreditor 2 |  |
| Other Government Department(OGD) Accreditor 1 |  |
| Other Government Department (OGD) Accreditor 2 |  |
| **CONTINUE FORM AS NORMAL** | | | | | |
| R0750.1 | You have now completed the RBC questionnaire. Once you are satisfied with your answers, please send this form back. | I confirm that:   * I am an authorised representative of the organisation * I accept that I am accountable for the answers that I have provided and that they represent a true and honest account * No information has been omitted which should reasonably have been shared * In entering this data, I have abided by the DART Security Operating Procedures | |  |  |
| I confirm that this submission does not exceed OFFICIAL-SENSITIVE. | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| R0750.3 | Please provide any additional information that you feel might be of use to the Approving Authority and stakeholders and/or respond to any comments that have been made previously. |  |  |