Security Operating Procedures (SyOPs)

Introduction

This document constitutes the Security Operating Procedures (SyOPs) for all Metaverse VR Ltd (MVR) applications. They are issued by the Information Technology Security Officer (ITSO) in accordance with the MOD Secure by Design Policy.

All MVR employees are to read, understand and observe MVR SyOPs. Deviation from or amendments to the MVR SyOps are not permitted unless, authorisation is gained in advance through MVR's ITSO and MOD CyDR Accreditor.

By logging on to MVR's information management systems all employees agree to follow the security instructions detailed in these SyOPs.

Disciplinary action may be taken against employee who break or ignore the SyOps. Any incident that has or is likely to compromise MVR security should be reported immediately to MVR's IT Manager and or the ITSO.

Scope

Role and Description of the System

MVR Information Management System (IMS), is the principal information system, used by MVR. The IMS is a suite of applications to enable the administration of MVR business through IT.

The IMS provides a single common set of managed applications which are monitored by MVR's IT Team.

These SyOps apply to the following applications

- MVR Intranet
- Remote Connectivity (inc but not limited to VPN, Mobiles, Tablets and laptops)
- Office 365 suite of applications
- All other software installed or accessed by MVR staff and third parties

Metaverse VR Users (MVR Users)

Throughout this document MVR will refer to a group of individuals who can access the applications listed above as MVR Users. To avoid confusion, a user is included in the term MVR Users if they belong to one or more of the following groups

- Metaverse VR Permanent Employees
- Metaverse VR Contractors
- MWorks Permanent Employees
- MWorks Contractors

Sensitivity Labelling

Level of Sensitivity Labelling

MVR processes and stores information at Official-Sensitive Personal. However, if the information contains Personal Identifiable Information (PII) it warrants additional protections to comply with the Data Protection Act 2018 – General Data Protection Regulation (GDPR).

Responsibilities

MVR User security responsibilities are as described in these SyOPs.

Personnel Security

Security Clearance Level & Access

All MVR Users will be cleared to minimum, Baseline Personnel Security Standard (BPSS), subject to random audit by the MVR ITSO.

All MVR Users are required to hold Enhanced Disclosure and Barring service (DBS), subject to random audit by the MVR ITSO.

Access to MVR IT will not be granted until DBS & BPSS are completed.

Responsible for Information

The Cabinet Office directs all personnel who have access to sensitive MoD information to complete Cyber Security Best Practices Training.

MVR Users who have access to:

- MVR email
- MVR SharePoint
- OS Paper Files
- Any other associated documents or files

Are required to complete the Responsible for Information – General User Assessment mandatory training.

Note:

- Employees with access to MVR email, MVR SharePoint, OS Paper Files or any other associated documents or files – To complete the Responsible for Information Assessment (valid for 3 years)
- Employees that DO NOT have access to an MVR Accounts, MVR SharePoint, OS Paper Files, OS Paper Files or any other associated documents or files – No Further Action

Passwords

Password Policy

Maintaining the integrity of the MVR IT infrastructure is the responsibility of all MVR Users.

- MVR Users are responsible for safeguarding their passwords.
- Passwords must not be stored or recorded in a manner that makes them visible or susceptible to theft.
- MVR users must not share their passwords with anyone, except when explicitly requested by the MVR IT Manager or ITSO for service or repair purposes.

Password Policy – Technical Enforcement

To ensure a baseline level of security, MVR passwords must adhere to the following technical requirements:

- Passwords must be at least 8 characters in length.
- MVR User-created passwords must include at least 1 alphabetic character, 1 numeric character, and both uppercase and lowercase letters.
- Passwords must be reset at intervals not exceeding 90 days.
- New passwords must not be the same as the previous 3 passwords.
- Users will be locked out after three consecutive failed login attempts.
- Upon a password reset, users must change their password at the next login.

Password Policy – Prohibited Passwords

MVR Users must refrain from using easily identifiable passwords, the following types of passwords are prohibited:

- Dates (e.g., birthdates, anniversaries)
- Family names
- Telephone numbers
- Any other easily guessable personal characteristics, such as addresses, nicknames, role title ect

These guidelines help to prevent the use of weak passwords that could compromise security.

With the exception of shared accounts, MVR users are NOT to share MVR User account details with anyone, MVR Users are not to access accounts not assigned to them without prior written authority from the MVR ITSO.

Storage and Media Management

Media Handling and Marking

The export of MVR data is only permitted for legitimate business purposes and for conducting MVR operations.

In such cases, the following must be adhered to:

- Protectively marked information (classified as “Official” or above) saved to removable media must be encrypted using an approved encryption product.

MVR Users should refer to the product options listed in the Defence Information Assurance Notice (DIAN) 15 for guidance.

Disposal and Destruction of Media

- Data storage media that is no longer required must be disposed of or destroyed using an approved method. For specific guidance, refer to HMG Infosec Standard No.5 (IS5).

For further advice on approved methods of destruction consult the MVR ITSO.

Information Import & Export

- The import and export of MVR data will only occur when there is a justifiable business operations requirement.
- All imports and exports of MVR data will be audited for justification, the MVR ITSO will audit the justification for any MVR data export.

Acceptable Use & Monitoring

- MVR users must not tamper with security settings or attempt to access information they are not authorised to view.
- The use of MVR IT applications are, and will remain, subject to continuous monitoring. MVR Users are advised system logs are regularly reviewed to detect any unauthorised or suspicious security activity.
- Users must take care to ensure that MVR information is not visible to visitors, bystanders, or unauthorised employees.

MVR information must not be accessed from untrusted or public internet connections, such as Internet Cafes.

Incident Management & Reporting Security Breaches

All MVR Users have a responsibility to report security incidents. MVR Users must remain vigilant for potential or actual security breaches, which may include, but are not limited to:

- Compromise of user passwords
- Corruption of information
- Non-availability of information
- Loss or compromise of information

All potential or actual breaches must be reported to the MVR IT Provider and or the MVR ITSO. The MVR ITSO will escalate to the Air Warning and Reporting Point (WARP). MVR ITSO is responsible for informing the MOD CyDR Accreditor and the appropriate chain of command, in accordance with JSP 541.

Registered in England: 13684068, VAT No: GB 399750824.
Registered office: 3.05, Innovation and Collaboration Hub Portsdown Technology Park, North Hill Portsmouth, PO6 3RU
Tel: +44 (0) 2393 552 794 Email: info@metaverse-vr.co.uk