Ahead

MANAGEMENT GROUP

Security Policy

Building fair and effective standards into our business

Table of Contents

AheadMG Ltd 4th Floor, Silverstream House, 45 Fitzroy Street, Fitzrovia, London, W1T 6EB

Management@aheadmg.co.uk

Document Control

Document History

	Author	Version	Description
02/08/2013	Matt Westmacott	V0.1	Template Draft
02/08/2013	Matt Westmacott	v0.2	Initial AheadMG Draft
23/08/2013	Matt Westmacott	V0.3	Reviewed at board meeting, minor amendments.
27/09/2013	Matt Westmacott	V1.0	Baselined version
09/12/2013	Neil Hickman	V1.1	Access Controls Updates
12/13/2015	Andy Fox	V1.2	Incident Reporting Updates
17/03/2015	Andy Fox	V1.3	Reviewed and re-baselined
12/09/2018	Tracy Allen	V1.4 (Draft)	Draft - Added Text covering GDPR Updated AheadMG business address.
14/09/2018		V1.4 (Approved)	Latest Updates accepted at Exec Meeting
19/07/2019	Tracy Allen	V1.5 (Draft)	Minor updates for 2019
23/07/2019		V1.5 (Approved)	Latest Updates accepted at Exec Meeting
01/07/2020	Tracy Allen	V1.6 (Draft)	Minor updates for 2020
08/07/2020		V1.6 (Approved)	Latest Updates accepted at Exec Meeting
18/02/2022	Donna Chapman	V1.7	Minor updates for 2022
24/08/2023	Donna Chapman	V1.8	Minor updates for 2023

Signatories

Name	Role	Sign off Date
Andy Ewell	AheadMG Delivery Director	08/07/2020
Neil Hickman	AheadMG Finance Director	08/07/2020

Document Owner

The document is owned and maintained by the AheadMG Head of IT.

Document Storage

All versions of the policy will be stored on our website https://www.aheadmg.com/new-starters/

Introduction

Purpose

This document provides guidance to users of the computer systems of AheadMG. Implementation of the policies herein will ensure adequate security for all information collected, processed, transmitted, stored, or disseminated as part of AheadMG systems and major applications.

These security policies are consistent with UK Government legislation

General Security Policy and Standards

Objectives

To establish and maintain adequate and effective information security safeguards for users to ensure that the confidentiality, integrity and operational availability of AheadMG and internal and 3rd party client information is not compromised.

Sensitive information must be safeguarded against unauthorised disclosure, modification, access, use, destruction, or delay in service – also see AheadMG Data Classification Policy.

Each user has a duty and responsibility to other AheadMG staff members to comply with the information protection policies and procedures detailed in this document.

Security Policy Reviews

The standard and quality of the information security controls implemented at this AheadMG will be verified through periodic reviews to ensure compliance, including Director level periodic reviews.

Security Organisation

Policy Statements

A management framework is required so that all those involved in the use or maintenance of AheadMG computer systems can initiate, co-ordinate and control the implementation of information security effectively.

AheadMG Manager (Head of IT)

AheadMG Manager has a number of responsibilities with respect to the security of information, including:

- Establishing and approving information security policies and procedures
- Agreeing on specific methodologies and processes for information security, e.g. risk assessment, security classification, etc.
- Determining acceptable levels of security risks
- Monitoring major information security threats and incidents
- Approving major initiatives to enhance information security
- Ensuring that formal audits are performed as necessary
- Reviewing audit reports where security problems exist
- Appointing AheadMG Security Officer
- Acting as the Authorised Signatory in respect to the issuance of digital certificates

AheadMG Security Officer

AheadMG Security Officer is appointed by AheadMG Manager and is responsible for the co-ordination of security issues that affect AheadMG. In particular, AheadMG Security Officer is responsible for:

- Advising AheadMG staff on security matters
- Informing AheadMG Manager of any major security incidents
- Developing and reviewing security policies and plans to be approved by AheadMG Manager
- Maintaining a list of all persons authorised to have access to AheadMG premises, and to AheadMG computer systems
- Reporting security incidents, and the status thereof, to AheadMG Manager

Staff Responsibilities

Any security system relies on the users of the system to follow the procedures necessary for upholding security policies. AheadMG employees/associates are therefore expected to:

- Uphold security procedures and policies
- Protect their user identification and passwords
- Inform AheadMG Security Officer of any security issues, problems or concerns (see Incident Reporting Policy for details)
- Assist AheadMG Security Officer in resolving security issues
- Ensure that all computer systems used in support of AheadMG functions are backed-up in a manner that mitigates both the risk of loss and costs of recovery
- Be especially aware of the vulnerabilities presented by remote access and be aware of their obligation to report intrusions, misuse or abuse to AheadMG Security Officer
- Be aware of their obligations in the event that they are storing, securing, transmitting and disposing of health information to protect the privacy of patients

Risk Assessment

A formal risk assessment will be undertaken by AheadMG Security Officer no less often than at two yearly intervals.

It is not possible to eliminate all business risk; rather appropriate techniques should be applied to identify and manage the risks so as to minimise any harmful affects.

Security requirements will be identified by a methodical assessment of security risks. Expenditure on mitigating controls is to be balanced against the harm to AheadMG that is likely to result from security failures.

Risk assessment is the systematic consideration of:

- The harm likely to result from a security failure, taking into account the potential consequences of a loss of integrity, confidentiality and availability of the information and other assets
- The realistic likelihood of such a failure occurring in the light of the prevailing threats and vulnerabilities, and the controls currently implemented

The results of this assessment will assist in the determination of the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against those risks.

As a matter of course, security policies will be reviewed for currency and appropriateness following any assessment of risks.

Asset Classification and Control

Accountability for Assets

All major information assets should be accounted for and have a nominated owner.

Accountability for assets helps to ensure that appropriate protection is maintained. Owners are to be identified for each major asset and the responsibility for the maintenance of appropriate controls is to be assigned.

Inventories of assets help ensure that effective asset protection takes place, and will also be useful for other business purposes, such as health and safety, insurance or financial management reasons. The process of compiling an inventory of assets is an important aspect of risk management.

Information Classification

The following must be read in conjunction with the **AheadMG Data Classification Policy**.

Information is to be classified to indicate the need, priorities and degree of protection.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling.

An information classification system will enable the definition of an appropriate set of protection levels, and communicate the need for special handling processes.

The responsibility for defining the classification of an item of information, e.g., for a document, data file or disc, and for periodically reviewing that classification, is to be rest with the originator or nominated owner of the information.

Handling procedures are to be defined to cover:

- Copying
- Storage
- Transmission by post, fax and electronic mail
- Transmission by spoken word, including mobile phone, voicemail and answering machines
- Destruction

Personnel Security

Objectives

To ensure that employees are aware of information security threats and concerns, and are equipped to support AheadMG information protection policies and procedures in the course of their daily work.

Job Responsibilities

Security related roles and responsibilities are to be documented where appropriate in specific job descriptions.

Non-disclosure Information and Security Agreement

Contract staff and outside organisations not already covered by an existing contract (containing the confidentiality agreement) are required to sign a confidentiality agreement prior to accessing AheadMG facilities.

Training

Computer users must receive appropriate training before using computer facilities and applications used by AheadMG.

All employees of AheadMG are to receive appropriate training and regular updates in AheadMG policies and procedures, including security requirements, legal responsibilities and business controls.

See AheadMG Joiners Checklist for base training requirements including overview of our policies.

Note: 3rd Party specific training is also likely to be a requirement. Please speak to the AheadMG account manager for such matters.

Disciplinary Process

An appropriate disciplinary process is to be in place to cover both employees and contractors who may knowingly disregard a particular policy requirement.

To be reviewed in conjunction with the **AheadMG Disciplinary Policy and Procedure**

Physical Security

Policy Statements

All hardware, software, documentation and commercial information held by AheadMG is to be protected from disclosure, modification, or destruction. This is especially true if access may reveal information that can be used to eliminate, bypass, or otherwise render security safeguards ineffective.

Where identifiable Pii data and other sensitive information is stored, processed, or transmitted, physical access to that information is to be restricted to authorised individuals.

General Requirements

AheadMG operate a virtual office, therefore our policies are geared towards ensuring high integrity IT and virtual access controls, nonetheless individuals operating remotely at their own premises should follow best practice around management of physical security.

Areas in which information is stored are to be physically secure and access restricted to authorised personnel only. Access to documentation in respect to computer systems is also to be restricted to authorised personnel.

All persons, other than employees, who are granted access to AheadMG premises must be accompanied and their access restricted to those areas necessary for them to complete their tasks.

Clear Desk and Computer Screen Policy

Work areas are, as far as conveniently possible, to be kept clear of papers and removable storage media in order to reduce the possibility of unauthorised access, loss of, and damage to information during and outside normal working hours.

Similarly, screen savers are to be activated on all AheadMG computers.

The AheadMG standard desktop image must be used on all AheadMG laptops without exception.

Sensitive and critical AheadMG information, including computer media, is to be locked away when not required.

Equipment Protection

All items of equipment are to be sited or protected to minimise the risks from environmental threats and hazards, and opportunities for unauthorised access.

The impact of a disaster occurring in or around nearby premises is to be considered. Laptops must never be left overnight on a client site, unless there is a business requirement to do so and its supported by an adequate Kensington lock.

Work Performed Outside Secure Sites

Security controls are to be in place to ensure authorised operations and that sensitive information is properly protected.

Computers used to process HR information from remote locations must meet AheadMG security requirements and have authorisation from AheadMG Security Officer.

All data should be filed electronically. Any physical material must be scanned and saved onto the AheadMG system, with the original shredded.

Storage of Information

AheadMG information stored on computer systems must be regularly backed-up so that it can be restored if or when necessary.

Destruction of Information

All care and responsibility must be taken in the destruction of sensitive information.

Both paper and electronic information relating to administrative and commercial information must be disposed of in a secure manner.

Data Protection Act 2018 rules around persistence of data must be followed without exception.

Disposal of Storage Media

AheadMG information can be compromised through careless disposal of equipment. Accordingly, all sensitive information must be erased from computer storage media prior to disposal.

Similarly, no computer equipment that is sent or taken off-site for repair, should contain sensitive information.

Damaged storage devices such as hard disks may contain sensitive information that if disclosed could cause considerable embarrassment. Consideration should be given to not having a device repaired if information cannot be erased.

Computer Systems Access Control

Policy Statement

Access to computer services and information should be controlled on the basis of AheadMG requirements.

Responsibilities

Access control responsibilities are as follows:

AheadMG Manager

- Will determine and support AheadMG access control strategy
- Will ensure the satisfactory resolution of problems relating to the provision of user access when, in response to the concerns expressed by an AheadMG Security Officer, significant changes are deemed necessary

Designated Security Officer (AheadMG Senior Manager)

- Will ensure policies and standards address all AheadMG requirements and client requirements where required/applicable
- Will ensure that logon and system access procedures meet defined requirements
- Will ensure that data and applications are safe in project development environments
- Will assist users in their day-to-day use of AheadMG computer systems by performing basic account administration functions, including the unlocking of locked accounts, resetting passwords, providing user instruction

Guiding Principles to Access Controls

AheadMG will provide access privileges to its IT services (including networks, systems, applications, computers and mobile devices) based on the following principles:

- Need to know – users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities
- Least privilege – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities
- Formal Documented Requests - Requests for users' accounts and access privileges must be formally documented and appropriately approved
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by an appropriate manager

Information System Access Control

Minimum requirements for information system access control are:

- Valid individual user identifications and passwords for all computer access
- Successful and unsuccessful system accesses are to be recorded
- The last time a user was logged on is to be recorded or displayed
- User account details are to be issued at a formal training session (or with appropriate training materials if remote)
- New user accounts are to be initially configured so as to force a change of the password upon first logging on

User Logon Procedures

Access to AheadMG computer facilities are to be via a secure logon process. The relative logon procedure will:

- Not display system or application prompts until the logon process has been successfully completed
- Not provide help messages during logon procedures
- Validate the logon information only on completion of all input data
- Allow only three unsuccessful logon attempts before:
    - Recording the unsuccessful attempt
    - Forcing a time delay before further logon attempts are allowed
    - Suspending a user account to prevent repeated invalid access attempts
    - Disconnecting and giving no assistance after a rejected attempt to logon
- Limit the time allowed for the logon procedure; if exceeded, the system should terminate the logon
- Display the following information on completion of a successful logon:
    - Date and time of the previous successful logon
    - Details of any unsuccessful logon attempts since last successful logon

This allows the user to check whether it was that he/she who was last logged on. If not, the incident should be reported and appropriate action taken.

Password Standards

The following password standards are to be adhered to ensure compliance with the basic principles of logical security:

- The use of individual passwords is to be enforced to maintain accountability. Sharing of passwords is NOT permitted
- Users should be able to select and change their own password and be required to provide a confirmation to account for typing errors
- A password is to have a minimum length of eight characters
- Passwords are not to be based on any of the following:
    - Months of the year, days of the week or any other aspect of the date
    - Family names, initials or car registration numbers
    - Company names, identifiers or references
    - Telephone numbers or similar all-number groups
    - User identification, user name, group identification or other system identifier
        - more than two consecutive identical characters
        - all-numeric or all-alphabetic groups
        - any word contained in a dictionary, either English or another language
- Maximum password lifetime is to be 90 days for normal user accounts and 60 days for system administrator accounts
- Users are to be forced to change temporary (initial) passwords at the first logon
- Passwords are not to be displayed while being entered
- Password files should be stored separately from the main application system data, and any access restricted to the system administrator
- Password files are to be stored in encrypted form, using a one-way encryption algorithm

Individual User Account Management

Periodic reviews of all user accounts are completed. Inactive user accounts that are no longer required are to be disabled and identified as pending deletion.

An AheadMG Security Officer is required to approve the continued availability of a particular inactive user account.

Electronic Mail

As electronic mail (e-mail) is a business resource, AheadMG personnel are to note that:

- Personal use of e-mail is to be kept to a minimum
- The e-mail system is inherently insecure and individuals other than the intended recipients may be able to read messages
- Nothing should be included in an e-mail message that would not be printed on AheadMG letterhead
- The information contained in e-mail messages forms part of AheadMG business records
- No sensitive information should be sent as part of, or attached to, an e-mail message unless the information is encrypted
- E-mail attachments are a common source of malicious software and particular care is to be taken before opening any attachments, especially if the message is not from a trusted source
- Management reserves the right to monitor the content of e-mail messages

All personnel should be aware of the security risks created by electronic mail including the vulnerability of messages and any legal considerations.

Employees and associates should not use their own email addresses for any AheadMG or connected 3rd Party business.

External Network Connections and Controls

Connections to other networks, including the World Wide Web, are to be protected through a firewall.

Firewalls must be properly configured so as to ensure the required level of security is achieved.

Default settings in network servers are to be changed so as to minimise the possibility of unauthorised access.

No software, or other material, is to be downloaded from the World Wide Web without the prior knowledge and agreement of an AheadMG Security Officer.

Security in System Life Cycle Management

Installation of Software

An AheadMG Security Officer is to approve all software prior to it being installed.

All AheadMG laptops are configured to have separate Admin right user roles, restricting the amount of additional configuration an employee / associate can make. IT Security / Helpdesk have access to Admin right passwords only.

Operational Software

Vendor supplied software used in operational systems is to be maintained at a level supported by the supplier.

Software patches that help to remove or reduce security weaknesses are always to be applied in a timely manner and with appropriate consideration for the seriousness of the risk an unpatched vulnerability poses.

Technical Support and Maintenance

Hardware and software maintenance activities are not to affect the integrity of existing safeguards or permit the introduction of security exposures (computer viruses, logic bombs, malicious code, etc.) into the AheadMG computer systems.

Automated dial-up diagnostic maintenance of sensitive applications by software vendors via remote communications is only to be undertaken under the direction of an AheadMG Security Officer.

Computer Integrity and Incident Reporting

Policy Statements

All personnel are to comply with the software integrity procedures outlined in this document especially in respect to the following:

- Security violations and software malfunctions reporting
- Virus prevention and monitoring

Security Incident

A security incident is an event and/or condition that has the potential to impact on security or privacy and may result from either intentional or inadvertent action.

All employees, and others likely to be involved, are to be made aware of the procedures for reporting incidents that might have an impact on the security of AheadMG assets and information.

Security Violation

A security violation is an event that may result in disclosure of sensitive or otherwise classified information to unauthorised individuals, or in unauthorised modification or destruction of system data, loss of computer system processing capability, loss, or theft of any computer system resources.

If a security violation occurs as a consequence of a user's access, that user and any like users are to be provided with guidance by an AheadMG Security Officer to ensure that the violation does not re-occur.

Reporting of Security Incidents or Weaknesses

Systems should be monitored to detect deviation from access control policy and record events to provide evidence in case of security incidents. System monitoring allows the effectiveness of adopted controls to be checked and conformity to access policies to be verified.

Similarly, unauthorised intrusions are to be monitored.

Any security-related incidents, violations or weaknesses, are to be reported to an AheadMG Security Officer at the earliest possible time but by no later than the following business day.

Malicious Software

Software and information processing facilities are vulnerable to the introduction of malicious software such as computer viruses, network worms and Trojan horses. It is therefore essential that precautions are taken to both detect and prevent the introduction of malicious software.

Virus Prevention Procedures

New viruses are being developed at regular and frequent intervals and could seriously undermine the integrity of the AheadMG systems unless they are prevented. Accordingly, all workstations are to have anti-virus software installed.

An AheadMG Security Officer needs to ensure that virus signature files are updated on a regular (no less frequently than monthly) basis so as to ensure that any new viruses can be promptly identified and removed.

Each individual user must ensure that the anti-virus software is active on their workstation so that any potential viruses from external sources are identified and removed.

Virus Education Programmes

All users are to receive basic training as to how best prevent the introduction of computer viruses and other malicious software.

An AheadMG Security Officer is to therefore ensure that:

- Users are aware that e-mail attachments may contain (often unknown) viruses or other malicious software.
- Users immediately report attachments with suspicious file extensions (including .vbs, .shs, .pif and .exe) to the organisation's IT support help desk.
- Users know to never launch e-mail attachments from their e-mail systems unless received from a trusted source, and then only after due care has been taken.

Disciplinary procedures are to be brought into play in the event that a user fails to follow designated malicious software procedures.

Web Security

Policy Statements

All personnel are to comply with the Web Security procedures outlined in this document especially in respect to the following:

- Identifying and reporting internal and external Web security threats
- Active input into the mitigation and risk reduction for all AheadMG users

Web Security Risk Appetite Statement

AheadMG has a tolerance for risk, allowing it to achieve its business goals and objectives in a manner that is compliant with the laws and regulations in the jurisdiction in which it operates.

- AheadMG has a low appetite for the loss or breach of its business and customer data in pursuit of its goals
- AheadMG has a low risk appetite for physical information security assets and will track assets greater than £500
- Information assets will be protected per AheadMG data classification policy
- AheadMG as a low risk appetite for access controls. All access to AheadMG mission-critical systems will be controlled via Information Security Policy

Social Engineering

The Social Engineering Awareness guidelines is a set of principles and practices for employees and contractors of AheadMG.

In order to protect AheadMG's assets, all employees and contractor need to defend the integrity and confidentiality of AheadMG and all client resources.

These guides have two purposes:

i) To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks
   - Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks
   - Employees know who to contact in these circumstances
   - Employees recognize they are an important part of AheadMG's security. The integrity of an employee is the best line of defence for protecting sensitive information regarding AheadMG or client resources

ii) To create specific procedures for employees to follow to help them make the best choices when:
   - Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect AheadMG or client sensitive information
   - The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data

Scope

Includes all employees of AheadMG, including temporary contractors or part-time employees participating with help desk customer service.

Social Engineering Techniques

Sensitive information of AheadMG or its clients will not be shared with an unauthorised individual if he/she uses words and/ or techniques such as the following:

- An "urgent matter"
- A "forgotten password"
- A "computer virus emergency"
- Any form of intimidation from "higher level management"

- Any "name dropping" by the individual which gives the appearance that it is coming from legitimate and authorized personnel
- The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of <Company Name> resources
- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person
- The techniques are used by a person that declares to be "affiliated" with <Company Name> such as a sub-contractor
- The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company
- The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger)

Guideline Actions

If one or more circumstances described in above is detected by a person described in the scope, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.
If the identity of the requester CANNOT be promptly verified, the person MUST immediately contact his/her AheadMG manager (and/or Client Manager if applicable).
If the supervisor or manager is not available, that person MUST contact another senior AheadMG manager.
If an appropriate Manager or Senior Manager is not available, the person must immediately drop the conversation, email, online chat with the requester, and report the episode to his/her Manager before the end of the business day.

Policy Compliance

Compliance Measurement

The AheadMG Security Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the AheadMG Security Manager in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web Security Risk Assessment

A Web security risk assessment identifies the information assets that could be affected by a cyber-attack (such as hardware, systems, laptops, customer data and intellectual property). It then identifies the risks that could affect those assets.

AheadMG will perform a Risk evaluation, followed by the identification and implementation of risk controls and mitigations. The process will map the risks against a standard risk matrix taking into account probability as well as impact of the risk materialising.

The risks will be monitored and reviewed regularly including ad hoc reviews at times of significant organisational or environmental change at AheadMG or its operating domain.

Web Security Knowledge and Training

It is essential that AheadMG employees and associates understand Information security risks and concepts. Please review the Information Security Policy and Induction material and ensure you understand its contents – this includes intro to web security from the Open University.

Business Continuity Management

An AheadMG Business Continuity Management plan is to be implemented so as to minimise the effects of disruption caused by disasters and system failures (which may be the result of, for example, natural disasters, equipment failures, or deliberate actions) through a combination of preventative and recovery controls.

Plans are to be developed and implemented to ensure that AheadMG processes can be restored within the required time-scales, and are to be maintained and practised so as to become an integral part of all other management processes.

The key elements of business continuity management include:

- Understanding the risks, the organisation faces in terms of their likelihood and their impact, including identification and prioritisation of critical business processes
- Understanding the impact which interruptions are likely to have on the AheadMG
- Establishing the business objectives of information processing facilities
- Considering the purchase of suitable insurance which may form part of the business continuity process
- Formulating and documenting a business continuity strategy consistent with AheadMG objectives and priorities
- Formulating and documenting business continuity plans in line with agreed strategy
- Regular testing and updating of the plans and processes put in place
- Ensuring that the responsibility for managing business continuity is clearly defined in the AheadMG's processes and structure

Compliance

Software Licence Compliance

All conditions of a vendor's software licence are to be strictly observed.

Users are responsible for ensuring that all licensing obligations are met and maintained.

Security Awareness

All users are to be kept aware of their general security responsibilities and be regularly updated. It is essential that users understand and adhere to procedures for managing, detecting and responding to security incidents.

An AheadMG Security Officer is to take responsibility for maintaining user security awareness.

Compliance with Security Policy

All security procedures are to be subject to periodic review so as to ensure compliance with AheadMG security policies and standards.

Similarly, information systems are to be checked for compliance with security implementation standards.

Audits of operational systems are to be planned and agreed so as to minimise risk of disruption to AheadMG processes.

Approved Non-Compliance

Where a particular policy cannot be complied with for a substantive business reason, approval for a deviation from policy is to be obtained from an appropriate AheadMG Senior Manager.

Requests for authorised non-compliance must be formally submitted with details of any risks associated with the deviation.

An AheadMG Security Officer will maintain a record of all approved non-compliance requests.

All approved non-compliance requests will be subject to six-monthly reassessments.