PROTECTED DATA COMMUNITY ENVIRONMENT (PDCE)

COMMUNITY RULES INFORMATION SECURITY POLICY (CRISP)

JANUARY 2019

AUCLOUD

AUC-POL-048

Protected Data Community Environment (PDCE) Community Rules Information Security Policy (CRISP)

1. POLICY OVERVIEW

1.1. Sovereign Cloud Australia (AUCloud) provides an infrastructure to enable clients to host data and applications in a secure and resilient manner. The AUCloud platforms are designed to meet the controls of PROTECTED as documented within Australia Signals Directorate's (ASD) Information Security Manual 2017 (ISM) and will meet the accreditation and assurance requirements associated with data at these levels. The resulting Infrastructure-as-a-Service (IaaS) compute and storage services enable users (and their Chief Information Security Officers) to host their data within environments that mitigate the underlying risks associated with data that they have assessed as Unclassified with a dissemination limiting marker (DLM) or PROTECTED as per the Protective Security Policy Framework (PSPF).

By definition, National Institute for Standards in Technology (NIST) based cloud services are designed with distinct separations of ownership of the overall environment. Essentially, AUCloud provides and owns the infrastructure that supports the applications and data, whilst the clients own and have responsibility for, their individual applications, system configurations and associated data.

This separation of ownership also includes a separation of security ownership, accountability and responsibility. The AUCloud environment will meet the controls as specified in the Information Security Manual (ISM) as well as achieving applicable accreditations, certifications and supporting assurance validations. To meet these criteria, it is necessary to identify the overall security requirement and then to agree the ownership, accountability and responsibility boundaries between AUCloud and its clients.

This Community Rules Information Security Policy (CRISP) is the formal, top-level security document, which identifies those aspects that are within the remit of the AUCloud Chief Information Security Officer (CISO) and Information Technology Security Advisor (ITSA) and those that are within the remit of the data-owning client's CISO and ITSA. Specific information is contained within the SyOPs sections of the appropriate RMADS documentation issued for each individual AUCloud service.

AUCloud IaaS is provided for the benefit of Australian Government (Federal, State and Local) including related entities and charitable organisations, Critical National Industries including Banking and Finance, Communications, Energy, Health, Transport and Water services, as well as organisations providing services to or on behalf of Government and Critical National Industries.

This CRISP addresses the responsibilities and required behaviours for customers and their users of AUCloud's Community Environment that is designed to support data that customers have classified as PROTECTED in line with ASD's ISM. Acceptance of this PDCE CRISP is agreement to comply with the separation of security requirements and responsibilities.

2. SECURITY POLICY

2.1. The PDCE CRISP, while being the overarching security policy for the AUCloud environment, does not address individual security requirements in detail. AUCloud shall provide corresponding security documentation for the infrastructure and the client shall provide similar documentation for their individual applications and data.

2.2. AUCloud has communicated the detailed security requirements of its services within the PDCE RMADS documentation. The PDCE RMADS documentation is provided to the end client's CISO/ITSA prior to their deployment and consumption of the AUCloud service, and the client remains at all times responsible for full compliance with the requirements of the SyOPs contained within the PDCE RMADS documentation.

2.3. Each party (AUCloud and the end client) shall make the other party aware of any salient aspects of their own security policy.

2.4. The PDCE CRISP and AUCloud Information Security Policy shall be reviewed annually as a minimum, and in the event of any security incident. Changes, if required, shall be informed to the client. It is expected that the client shall also review their security policy at least annually and any relevant changes will be informed to AUCloud promptly.

3. ORGANISATION OF INFORMATION SECURITY

3.1. AUCloud shall have designated Risk Owners and Security Officers with an overall Responsible Individual designated to own the security regime of each. The client shall have their own designated personnel in the relevant roles to own and co-ordinate their own security activities.

3.2. Formal processes shall exist between AUCloud and its customer, suppliers and where relevant, its channel partners to co-ordinate their security activities. The client shall ensure that relevant co-ordination exists with their areas of responsibility. Liaison and co-ordination between the client and AUCloud shall be agreed as part of the formal contract using this PDCE CRISP.

3.3. The initial configuration and composition of the overall system shall be agreed between AUCloud and the client. Any subsequent changes or additions to the system will be addressed through a formal Change Management Process and agreed with the applicable accreditation authority as applicable. AUCloud shall not make any changes to technology that it has responsibility for other than those that are known, approved and scheduled, or those considered necessary to complete emergency maintenance or address a serious security incident. The client shall ensure that any changes to their existing applications or data processing arrangements will be subject to the documented requirements of their own change management process.

3.4. The Protective Monitoring of the AUCloud Management Platform environments shall be implemented to identify and manage security incidents. AUCloud shall contact the relevant authorities (e.g. Australian Cyber Security Centre (ACSC) or AusCERT) in the event of any such incident as well as invoking the defined Incident Management Process. Clients shall be informed in the event of any such incidents in accordance with the agreed Incident Management Process,

using the client contacts notified within the Security Incident Reporting Matrix.

3.5. The client shall be responsible for complying with all applicable reporting requirements with respect to their applications and data.

3.6. The client shall promptly inform AUCloud when they detect any Security Incidents in accordance with the Incident Management Process. This shall include proactive notifications of current ongoing security incidents, and reactive notifications for previous security incidents.

3.7. AUCloud and the client shall agree with the relevant accreditation and certification bodies the frequency of review of any accreditation or certification status (if applicable).

3.8. AUCloud services will be assessed for risk using the International Organisation for Standardization (ISO) 27001 standard as part of AUCloud going through ASD's Information Security Registered Assessor Program (IRAP) security assessment. This risk assessment shall be reviewed annually to ensure that the risk situation is current and valid. There shall be additional assessments in the event of any major security incident. Any changes to the risk profile shall be informed to the client. The client shall conduct their own risk assessment and shall review their own assessment at least annually in line with ISM requirements.

3.9. AUCloud has responsibility for ensuring that the cloud infrastructure provides the relevant level of security, including Protective Monitoring (for the AUCloud Management Platform) and Incident Management. AUCloud shall also ensure that all personnel who have access to the infrastructure have obtained and retain a minimum-security clearance of Negative Vetting Level 1 (NV1) as defined by the PSPF.

3.10. The client shall have responsibility for ensuring that their applications and data are provided with the relevant level of security and that access to those applications and their data is restricted to those who require such access and who have obtained and retain a minimum-security clearance of Baseline as defined by the PSPF.

4. CONNECTIVITY OPTIONS

4.1. Access to the PDCE Management Portal is provided using geo-location services and restricted to Australian IP addresses. Access to the PDCE Management Portal is explicitly restricted to Australian IP addresses and any exceptions to control must be risk assessed and agreed between AUCloud and the client.

4.2. AUCloud shall provide the following connectivity options for clients connecting to the AUCloud PDCE platform:

- Direct fibre connection where a client resides in the same data centre facility;
- Network service provider where a client has a connection within an AUCloud data centre;
- Virtual Private Network (VPN) connection through the client's edge services gateway.

4.3. AUCloud shall provide suitable encryption options, typically IPSec or MACsec, to clients connecting to the AUCloud PDCE platform based upon the connectivity method selected.

Encryption technologies shall be implemented in line with the requirements of the ISM.

4.4. Clients connecting to AUCloud services shall provide confirmation that the client has deployed a security or protective monitoring solution in line with the requirements of the ISM. Where clients do not have a suitable solution then AUCloud's Protective Monitoring service will be utilised.

4.5. For clients connecting to the AUCloud PDCE platform, AUCloud shall maintain a whitelist of common inbound ports that are open as standard on the platform from the internet. The whitelist policy applies where connectivity is established using internet routable addresses. All outbound ports from a client environment are open by default. AUCloud and the client shall agree if any changes are required outside of the standard whitelist.

4.6. AUCloud shall operate enhanced network analysis and intrusion policies to ensure the protection of AUCloud platforms with security taking precedence over convenience.

5. ASSET MANAGEMENT

5.1. The AUCloud infrastructure comprises a number of separate environments, each designed for different sectors and employing different security controls. All elements of each environment shall be inventoried and classified to meet the stated requirements of the sector and data classification. All environments shall be assessed for security control effectiveness in relation to data Confidentiality, Integrity and Availability.

5.2. The client shall identify all of their assets to be used within and to access the AUCloud environment and will assess them to ensure their suitability with regards to data Confidentiality, Integrity and Availability.

5.3. AUCloud shall label and handle all management information assets that they have control of and responsibility for, in accordance with the sensitivity and/or protective marking of each asset.

5.4. The client shall have sole responsibility for the labelling and handling of their information assets, and any other assets associated with their applications. The client shall also be responsible for assessing and complying with their own data aggregation requirements, and for assessing if this aggregation affects their defined security levels. AUCloud assumes that clients will only deploy data that is classified as PROTECTED within the PDCE.

5.5. AUCloud shall be responsible for assessing the overall implications of aggregation of data across its cloud infrastructure.

6. PHYSICAL & ENVIRONMENTAL SECURITY

6.1. AUCloud shall have responsibility for ensuring that all physical and environmental controls are in place in those areas where the infrastructure, or management access to that infrastructure, is made. They are also responsible for ensuring that the relevant level of physical access controls to such areas is in place.

6.2. The client shall have responsibility for ensuring that the relevant security and physical access controls are in place at all locations where access to their data is made from.

6.3. AUCloud shall provide appropriate training, guidance and security controls to its personnel who are to undertake their duties within secure areas. The client shall be responsible for providing any training, guidance or security controls needed for its personnel working in secure areas where access to their applications and data is made from.

6.4. AUCloud shall be responsible for the siting and protection of equipment within the data centre environment. The client shall be responsible for the siting and protection of equipment within their own environment(s), which is used to provide access to their applications and data.

6.5. AUCloud shall maintain all equipment within their control. Such maintenance shall be conducted in a secure manner by personnel with a minimum-security clearance of NV1 as defined by the PSPF. The client shall be responsible for the maintenance of the equipment they use to access the AUCloud cloud environment and for the suitability and security clearance of personnel who conduct maintenance on their equipment to ensure a minimum-security clearance of NV1 as defined by the PSPF.

6.6. AUCloud shall ensure the security of off-site infrastructure (such as laptop computers and mobile devices) and the information that may be contained on them. Client data stored on AUCloud services shall not be stored on off-site equipment. Appropriate protection, in line with ISM requirements, will be provided for any transportable media.

6.7. AUCloud shall ensure the secure disposal, in line with ISM control requirements for PROTECTED data, of any equipment within their control that requires replacement. The client shall be responsible for the secure disposal or re-use of any equipment within their control that is used to hold or access secure data.

6.8. AUCloud shall ensure that the appropriate physical security, in line with PSPF requirements, is applied to prevent the removal of equipment or assets within their control. The client shall be responsible for the physical security of their equipment and information assets.

7. COMMUNICATION & OPERATIONS MANAGEMENT

7.1. AUCloud shall produce specific procedures for the function of the Management Platforms that supports the PDCE, which shall be combined into an overall AUCloud Standard Operating Procedures (SOPs) manual.

7.2. The client shall be responsible for the production of operating procedures for their use of the applications and data. The client shall be responsible for ensuring that such documentation is developed in line with ISM requirements.

7.3. AUCloud shall ensure that only its personnel have access according to their role within the PDCE Management Platform and that no potential conflict exists in the allocation of these roles. The client shall be responsible for ensuring that, where appropriate, the relevant segregation of duties is enforced within their own environment.

7.4. AUCloud shall continually manage and monitor the services provided by any third party provider to the AUCloud PDCE Management Platforms through the PDCE Protective Monitoring system. The client shall be responsible for ensuring that any services (including Protective Monitoring thereof) provided by their third parties are regularly managed, audited and assessed.

7.5. The services provided by AUCloud third parties shall be contractually defined. Any subsequent changes to these services shall be via Change Management. Significant changes shall be notified to and authorised by the appropriate accreditor or certification body, if applicable. The client shall be responsible for managing changes to the services provided by their third-parties and ensuring that AUCloud and, where relevant, their accreditor or certification body is informed.

7.6. AUCloud shall monitor and manage the capacity of the AUCloud PDCE Management Platforms. The client shall be responsible for monitoring and managing the specific capacity requirements of their own systems hosted on AUCloud PDCE infrastructure.

7.7. AUCloud shall ensure that the relevant controls against the introduction of viruses and malicious code are in place for the PDCE and the related PDCE Management Platform. The client shall be responsible for ensuring that they have appropriate and relevant controls in place to protect their environments and data from malicious code being introduced to their data.

7.8. AUCloud shall ensure that a Protective Monitoring service is in operation to provide protection to the AUCloud PDCE Management Platforms. Clients shall ensure that their environments are similarly protected by an appropriate Protective Monitoring service, which aligns with the protective monitoring controls contained within the ISM.

7.9. AUCloud shall ensure that a suite of data backup services and appropriate infrastructure are made available and supported so that clients can backup their data as required. The client shall be responsible for the selection and configuration of the data backup tools, which are required to address their specific data backup requirements.

7.10. AUCloud shall ensure that the relevant security controls are in place on the AUCloud PDCE Management Platform networks. The client shall be responsible for ensuring that their network, up to the point of accessing the AUCloud managed networks, has the relevant security controls (a) as identified by their own risk assessment activities, and (b) which align with the client requirements documented within the SyOPs of the RMADS for the AUCloud PDCE service. Additionally, the client's use of an ASD certified security gateway or direct fibre connectivity to access the AUCloud PDCE Management Platform shall be managed and operated strictly in accordance with the corresponding security controls as specified within the ISM and shall deploy encryption standards to those outlined within the ISM for PROTECTED data. As an alternative, ICON connectivity may also be used.

7.11. AUCloud shall ensure that appropriate security controls are in place to protect any media within its control, including the disposal of media that is no longer serviceable or which is no longer required, as well as the sanitisation or destruction of any data on such media. The client shall be responsible for the proper management and secure deletion of their data, which is located within the AUCloud PDCE.

7.12. AUCloud shall ensure that appropriate information exchange policies, agreements and procedures are in place within the Management Platforms. The client shall be responsible for establishing and implementing information exchange policies, agreements and procedures with respect to their own applications and data, which align with the client requirements documented within the SyOPs of the PDCE RMADS for the AUCloud PDCE.

7.13. AUCloud shall ensure that all user activity within the PDCE Management Platforms are audited and logged. Any anomalous behaviour shall be investigated. The client shall be responsible for the audit of user activity of their applications and data.

7.14. AUCloud shall monitor system use of the PDCE Management Platforms as part of any incident response or investigation. The client shall be responsible for monitoring system use as part of an incident response or investigation into the applications and data.

7.15. AUCloud shall be responsible for the protection of audit logs. The client shall be responsible for the protection of audit logs under their control relating to access to and use of their data.

7.16. AUCloud shall be responsible for the audit logs of users within the PDCE Management Platforms. The client shall be responsible for audit logs under their control, which record activities relating to users of the data.

7.17. Any system faults within the PDCE shall be logged and, depending on the category of faults, reviewed at defined intervals by AUCloud. The client shall be responsible for logging and reviewing faults associated with their applications.

8. ACCESS CONTROL

8.1. AUCloud shall not access client data or applications, unless specifically requested to do so by the client, and having received prior formal written approval for this access from the client. Access to the PDCE Management Platforms shall be defined according to the function of the individual AUCloud employee. The client shall be responsible for managing and controlling access to their data.

8.2. AUCloud shall be responsible for implementing a user registration procedure for personnel who access the PDCE Management Platform, and for undertaking reviews of the privileges and access rights of personnel who have such access. The client shall be responsible for implementing a user registration procedure for personnel who are to access their data and applications, and for undertaking regular reviews of the privileges and access rights of personnel who are to access them. Clients will also ensure that personnel authentication policy is aligned with ASD ISM best practice.

8.3. AUCloud shall be responsible for ensuring (a) the security of unattended user equipment, (b) the security of mobile devices (such as smartphones, laptops and tablet computers) and (c) the implementation of a clear desk and clear screen policy within AUCloud offices and data centre environments. The client shall be responsible for ensuring (a) the security of unattended user equipment, (b) the security of mobile devices (such as smartphones, laptops and tablet computers) and (c) the implementation of a clear desk and clear screen policy within the environment of personnel who have access to managing and controlling their data.

8.4. AUCloud shall not access client data or applications, unless specifically requested to do so by the client, and having received prior formal written approval for this access from the client. The client's Protective Monitoring system shall identify any specific access to client data or applications that it has been requested to report. The client shall be responsible for identifying such activities, which are to be monitored and reported.

8.5. AUCloud shall be responsible for ensuring that its personnel working remotely will only be able to do so in accordance with relevant ISM controls. The client shall be responsible for identifying any remote working function it may have and producing the relevant security procedures.

8.6. AUCloud shall be responsible for ensuring that personnel accessing its PDCE Management Platforms use only accredited and/or approved technologies, which are required by the controls underpinning the PDCE Platform. The client shall be responsible for ensuring that external connectivity into their services(s) is undertaken using only accredited and/or approved technologies, which are specifically noted within the SyOPs of the PDCE RMADS.

9. INFORMATION SECURITY INCIDENT MANAGEMENT

9.1. AUCloud shall operate an Information Security Incident Management Policy, which details the management, investigation and reporting of potential or actual breaches of the Confidentiality, Integrity or Availability of a company information asset (or a client data asset where the company is engaged in a contractual agreement to protect the client data) or of a supporting asset (upon which the security of information assets depend).

9.2. The client shall be responsible for the management and reporting of potential or actual information security breaches to their data and applications to their own relevant external bodies, aligned to the Mandatory Notifiable Data Breach legislation. The client shall be required to immediately notify AUCloud of all such incidents.

9.3. The client shall be responsible for ensuring that their personnel details recorded within the Security Incident Reporting Matrix are regularly checked for accuracy, and for the prompt reporting to AUCloud of any personnel changes that need to be made.

9.4. AUCloud shall operate an Information Security Incident Management Policy that details the requirement to identify, report and act upon any known or suspected weaknesses to information or supporting assets within the AUCloud PDCE Management Platforms. Such weaknesses may also be identified by periodic security assessments, including technical reviews, audits or penetration tests.

9.5. The client shall be responsible for the identification and reporting of known or suspected weaknesses within their applications, and for promptly reporting these to AUCloud.

9.6. AUCloud shall operate an Information Security Incident Management Policy that details the roles, responsibilities and procedures required for managing, reporting and resolving information security incidents. The client shall be responsible for defining roles and responsibilities and implementing procedures for the reporting, management and resolution of information security incidents arising within their applications and/or data.

9.7. AUCloud shall maintain overall responsibility for the management and operation of the AUCloud PDCE Management Platforms. It shall be fully monitored and protected by a Protective Monitoring Service, which includes the collection and retention of log files and user activity data for use within any subsequent forensic investigation. The client shall be responsible for the identification of information relating to their applications and data, which needs to be retained and made available for any subsequent forensic investigation.

10. BUSINESS CONTINUITY MANAGEMENT

10.1. AUCloud shall operate Business Continuity policies and procedures that ensure that the PDCE Management Platform will continue to operate in the event of an unplanned business interruption to meet the service levels contracted with its clients. These shall be validated either by the design of the PDCE and related PDCE Management Platform, or in some cases by focussed testing activities. The client shall be responsible for implementing business continuity arrangements to address any unplanned business interruptions that are directly and solely attributable to a failure of their applications, and any consequential unavailability of their data.

11. COMPLIANCE

11.1. AUCloud shall identify all applicable legislation, regulation and guidance relevant to its operations, including the PSPF and ISM, and is committed to full compliance with these. The client shall be responsible for identifying and complying with all applicable legislation and regulations that are appropriate for their own business.

11.2. AUCloud shall identify and implement controls to protect its intellectual property rights, including, but not limited to its systems, software, designs, configurations and documentation. The client shall be responsible the appropriate protection of the intellectual property rights associated with their applications and data.

11.3. AUCloud shall operate a Data Protection Policy and related procedures to ensure that personal information and personally identifiable information is at all times protected in accordance with the Australian Privacy Act 1988. The client shall be responsible for full compliance with the Australian Privacy Act 1988 in respect of personal data introduced into the AUCloud environment.

11.4. The client shall remain responsible for undertaking a Business Impact Assessment, in line with PSPF requirements, of their data that is to be processed by or stored within the AUCloud PDCE service.

11.5. AUCloud shall operate an Acceptable Use Policy, provide training to its personnel on the acceptable use of information systems, and shall retain log files and user activity data to ensure that such systems are only used for authorised purposes in an acceptable way. The client shall be responsible for ensuring that their authorised users do not misuse information processing facilities.

11.6. AUCloud shall be responsible for ensuring that network access to its PDCE Management Platform is protected by the use of encryption technologies outlined within the ISM suitable for data classified to PROTECTED. The client shall be responsible for ensuring that external

connectivity into their services(s) is undertaken using similar technologies or alternative network connectivity solutions (e.g. Secure Internet Gateway, ICON) and as specifically noted within the SyOPs of the PDCE RMADS.

11.7. AUCloud shall have periodic (no less than annual) reviews of compliance with their security policies, processes and procedures as identified in the ISM. The client shall be responsible for assessing compliance with their own policies and for informing AUCloud and the accreditor of the results.