OPERATOR AGREEMENT / ADDENDUM
***(template*)**

between

_____
(Hereinafter referred to the Company)
(NOTE: The Responsible Party is here defined as the Company)

and

_____
(Hereinafter referred to as the "Operator")

---

1. INTRODUCTION

1.1 There are a variety of Personal Information privacy laws around the world which regulate the processing of Personal Information, including the General Data Processing Regulation (GDPR) in the EU and the UK and the Protection of Personal Information Act, 4 of 2013 (POPIA) in South Africa which as its main function and objective, regulates and controls the processing of Personal Information by a Responsible Party.

1.2 The Company, for the purposes of carrying out its business and related objectives, does and will from time to time, processes Personal Information belonging to several persons, including legal entities and individuals, who are referred to as Data Subjects under POPIA.

1.3 The Company is obligated to comply with POPIA, and the Data Protection conditions housed under POPIA with respect to the processing of all and any Personal Information pertaining to all and any Data Subjects.

1.4 In order for the Company to pursue its mandate and its related operational and business interests, the Company may from time-to-time request third parties to process certain Personal Information on its behalf, which Personal Information it has obtained from its Data Subjects.

1.5 In terms of section 20 of POPIA, where a Responsible Party makes use of the services of an Operator, to process Personal Information of Data Subjects on its behalf, then the Responsible Party is legally obliged to conclude a written agreement with such Operator, which written agreement contractually obliges the Operator to:

1.5.1 comply with the provisions of POPIA and the POPIA processing conditions when processing such Personal Information on behalf of the Company;

1.5.2 only process the Personal Information received from the Company in accordance with the mandate or written instruction received from the Company;

1.5.3 keep all the Personal Information held by the Operator on behalf of the Company and or belonging to the Company Data Subjects, confidential;

1.5.4 put measures in place to keep all such Personal Information held by the Operator, and

processed on behalf of the Company confidential, safe, and secure from misuse, abuse and or unauthorised use or access.

1.6 The Company is desirous of providing the Operator with certain Personal Information which pertains to certain of its Data Subjects, which the Company would like the Operator to process on its behalf, and the Operator has agreed to process the Personal Information on behalf of the Company, which processing will be subject to the terms and conditions set out under this Operator Agreement.

2. DEFINITIONS

2.1 The parties must take note of the following definitions, which will be used throughout this Operator Agreement, unless the context indicates a contrary meaning:

2.1.1 **"Agreement"** means the mandate or contract, or series of contracts entered between the Company and the Operator;

2.1.2 **"Company"** shall mean ..... who has mandated the Operator to process certain Personal Information belonging to Data Subjects, on its behalf, and in accordance with the terms of this Operator Agreement. (The Company being the Responsible Party in this Operator Agreement);

2.1.3 **"Data Subject (s)"** means the person (s) who own (s) the Personal Information which is to be processed by the Operator, on behalf of the Company, in terms of the Agreement and the Operator Agreement;

2.1.4 **"Operator"** (under GDPR means Data Processor) defined under POPIA means any person who processes Personal Information on another's behalf as a sub-contractor, in terms of an Agreement, without coming under the direct authority of the person requesting the processing;

2.1.5 **"Operator Agreement"** means this Operator Agreement;

2.1.6 **"person"** means an identifiable, living, natural person, or an identifiable, existing juristic person;

2.1.7 **"Personal Information"** means personal information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:

- **in the case of an individual:**
  - name, address, contact details, date of birth, place of birth, identity number, passport number, bank details, details about your employment, tax number and financial information;
  - vehicle registration;
  - dietary preferences;
  - financial history;
  - information about next of kin and or dependants;
  - information relating to education or employment history; and
  - **Special Personal Information** including race, gender, pregnancy, national, ethnic, or

social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

- **in the case of a juristic person:**
  - name, address, contact details, registration details, financials and related history, B-BBEE score card, registered address, description of operations, bank details, details about employees, business partners, customers, tax number, VAT number and other financial information; and
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.1.8 **"process or processing"** means any operation or activity or any set of operations, whether by automatic means, performed by the Operator concerning a Data Subject's Personal Information, including—

(a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure, or destruction of information;

2.1.9 **"record"** means any recorded information—

(a) regardless of form or medium, including any of the following:
  (i) writing on any material;
  (ii) information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
  (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  (iv) book, map, plan, graph, or drawing;
  (v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
(b) in the possession or under the control of a Responsible Party;
(c) whether or not it was created by a Responsible Party; and
(d) regardless of when it came into existence.

2.1.10 "**Responsible Party**" (under GDPR means "Data Controller") under POPIA means the person who is processing a Data Subject's Personal Information and who may under certain circumstances ask an Operator or Data Processor to process Personal Information on its behalf under and in terms of an Operator Agreement (which in GDPR is referred to as a Data Processor Agreement).

3. MANDATE TO PROCESS

The Company hereby grants to the Operator a mandate to process certain Personal Information, *identified under **Annexure A** on its behalf for the purpose and period set out under **Annexure A.***

4. OBLIGATIONS OF THE OPERATOR

4.1 The Operator expressly warrants and undertakes that it will:

4.1.1 process the Personal Information strictly in accordance with this Operator Agreement read together with **Annexure A,** any Agreement concluded between the Operator and the Company, and any specific instructions provided to it by the Company from time to time*;*

4.1.2 not use the Personal Information for any other purpose, save for the purpose set out under **Annexure A,** any Agreement concluded between the Operator and the Company, and any specific instruction provided by the Company from time to time**.**

4.1.3 only disclose, transfer and or hand over the Personal Information to those persons(s) identified under **Annexure A** and when transferring the information ensure that it has in place written arrangements which compel the identified party receiving the information to respect and maintain the confidentiality and security of the Personal Information and that said party has signed the POPIA transmission notice attached as **Annexure B**.

4.1.4 save for the provisions housed under clause 4.1.3, treat the Personal Information as confidential and not disclose the Personal Information to any other person unless required by law and only once it has provided the Company with adequate warning of this requirement to disclose and the related details thereof, including the identity of the person who is to receive the Personal Information, the reason for the disclosure and confirmation that the person to whom the Personal Information is to be disclosed to, has signed the POPIA onwards transmission notice attached hereto marked **Annexure B.**

4.1.5 has and will continue to have in place, appropriate technical and Organizational measures to protect and safeguard the Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which in addition, provides a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected and which safeguards comply with the requirements set out under POPIA, which measures are in line with the requirements described under the attached the Company Security Service Level Requirements, marked **Annexure C (**OPTIONAL**)**;

4.1.6 notify the Company immediately where it has reasonable grounds to believe that the Personal Information, which has been provided to it, including any Personal Information which it has processed, has been lost, destroyed, or accessed or acquired by any unauthorised person;

4.1.7 process the Personal Information strictly in accordance with POPIA and the POPIA processing conditions;

4.1.8 not use the Personal Information for any direct marketing or advertising, research, or statistical purposes, *unless expressly authorised to do as prescribed in its mandate and where applicable the Agreement / as described under* ***Annexure A*** and when conducting such activity ensure that this is done strictly in compliance with the requirements of POPIA and its regulations especially those applicable to direct marketing detailed under section 69;

4.1.9 not treat the Personal Information as its own, it expressly acknowledging that it has been tasked with processing the Personal Information in its capacity as the Company's Operator and agent, and that ownership of all the records housing the Personal Information and any records comprising such Personal Information pertaining to the Data Subject, will always remain with the Company;

4.1.10 not sell, alienate, or otherwise part with the Personal Information or any of the records housing the Personal Information;

4.1.11 where it is allowed to transfer the Personal Information onwards in terms of the Agreement or as per **Annexure A** to any third party, known as a Sub Operator, for the purposes of performing its mandate, ensure that such party concludes a "Sub Operator agreement" with it and the Company which compels the third party receiving the Personal Information to respect and maintain the confidentiality and security of the Personal Information, which Sub operator agreement will house the same terms and conditions as contained in this Operator Agreement, and which shall be concluded before the Personal Information is transferred to the Sub operator.

4.1.12 ensure that any person acting under the authority of the Operator, including any employee or sub operator, shall be obligated to process the Personal Information only on instructions from the Operator and strictly in accordance with this Operator Agreement, read together with the Agreement and in particular the Sub Operator Agreement, where applicable.

4.2 The Operator warrants that it has the legal authority to give the above-mentioned warranties and fulfil the undertakings set out in this Operator Agreement.

4.3 The Company, in order to ascertain compliance with the warranties and undertakings housed under this Operator Agreement, will have the right on reasonable notice and during regular business hours, to view and or audit, either by itself or through an independent agent, the Operator's facilities, files, and any other data processing documentation needed for the required review, audit and or independent or impartial inspection and the Operator undertakes to provide all necessary assistance which may be needed to give effect to this right.

5. LIABILITY OF THE OPERATOR AND THIRD-PARTY RIGHTS

5.1 In the event of the Operator breaching any of the warranties and undertakings housed under this Operator Agreement, then in such an event, the Operator shall be liable for all damages it may have caused in consequence of said breach, including patrimonial, non-patrimonial and punitive

damages suffered by the Company and or the Data Subject(s) and the Operator indemnifies and holds the Company and or any third party in consequence of said breach, harmless against all and any such loss, liabilities or damages, including pecuniary, non-pecuniary and or aggravated damages which may be incurred as a consequence of such non-compliance, the Operator agreeing to pay to the Company and or such third party all and any such damages on demand.

5.2 At the request of the Company, the Operator will provide the Company with evidence of financial resources sufficient to fulfil its responsibilities set out under this Operator Agreement which may include insurance coverage or other forms of collateral.

6. APPLICABLE LAW

The laws of South Africa shall apply to this Operator Agreement, regardless of where the Personal Information is, will be, or was processed.

7. TERMINATION

7.1 In the event of:

7.1.1 the processing of the Personal Information by the Operator has been completed in accordance with the Agreement;

7.1.2 the transfer of Personal Information to the Operator being suspended by the Company for longer than one month, for whatever reason;

7.1.3 the Operator is in breach of its obligations under the Agreement or this Operator Agreement and has failed when called upon to do so by the Company to rectify the breach or area of non-compliance;

7.1.4 the Operator is in substantial or persistent breach of any warranties or undertakings given by it under the Agreement or this Operator Agreement, notwithstanding that the Company has not given the Operator notice of such breach;

7.1.5 an application is filed for the placing of the Operator under business rescue, under administration, or winding up whether interim or final, which application is not dismissed within the applicable period for such dismissal under applicable law; or any equivalent event in any jurisdiction occurs,

then the Company without prejudice to any other rights, which it may have against the Operator, shall be entitled to terminate the Agreement and the Operator Agreement as well as the Sub Operator Agreement.

7.2 The Parties agree that the termination of the Agreement and the Operator Agreement at any time, and or the Sub Operator agreement, where applicable, in any circumstances and for whatever reason, does not exempt them from the rights and obligations set out under this Operator Agreement with regards to the processing of the Personal Information detailed under **Annexure A** read together with the obligations under POPIA.

7.3 In the event of the Agreement and or Operator Agreement being terminated whenever, and for

whatsoever reason, the Operator undertakes to:

7.3.1 restore and or transfer back to the Company all and any Personal Information which has been provided to the Operator for processing, including that held by the Sub Operator, whether same has been processed or not, and or which has been processed, together with any related documentation and or information, all of which documentation must without exception, be returned to the Company within a period of 30 (thirty) days from date of service of the termination notice.

7.3.2 to confirm in writing simultaneously when the transfer under clause 7.3.1 takes place, that all such Personal Information will be kept confidential as per the provisions of clause 4.1 and that it will not under any circumstances use the aforementioned information for whatsoever reason.

7.4 Notwithstanding termination of the Agreement and or the Operator Agreement and for whatsoever reason, the clauses 4, 5, 6 and 7.2 will survive any such termination.

8. GENERAL

8.1 Variation
The parties may not modify the provisions of this Operator Agreement including the information in **Annexure A, B or C** (OPTIONAL) unless such variation is reduced to writing and signed by the Parties.

8.2 The Operator Agreement forms part of the Agreement.

In the event of any conflict or inconsistency between the terms of the Agreement and the Operator Agreement, the terms, and conditions in so far as the processing of the Personal Information is concerned, as set out under this Operator Agreement will take precedence and govern its interpretation, application, and construction.

8.3 Notices

All notices to be provided in terms of the Operator Agreement must be sent to the Information Officer at: information.officer@bidvest.co.za

Concluded on ……at …….

_____
The Company

Concluded on ……at …….

_____
The Operator

ANNEXURE A

MANDATE TO PROCESS

DESCRIPTION OF THE PERSONAL DATA WHICH THE OPERATOR WILL PROCESS

Purpose(s):

.....

Description of the Personal Information belonging to the Data Subject(s) which the Operator has been asked to process in terms of this Operator Agreement

.....

PERSONAL DETAILS	**MANNER AND FORM AND RECORD DETAILS**
General	
☐ Name ☐ Identifying number ☐ Age ☐ Birthdate ☐ Language ☐ Physical and postal address ☐ e-mail address ☐ Telephone number ☐ Location information ☐ Other identifiers ☐ Gender ☐ Marital status ☐ Vehicle registration number	
Race and gender	
☐ Gender ☐ Race ☐ Colour ☐ Ethnic origin ☐ National origin	

Religion and belief	
☐ Religion ☐ Conscience ☐ Belief ☐ Culture	
Sexual orientation	
☐ Sex ☐ Sexual orientation	
Deviant behaviour and Criminal history	
☐ Criminal history	
Education	
☐ Education history ☐ Employment history ☐ Psychometrics	
Physical and medical	
☐ Medical history ☐ Physical health well-being ☐ Pregnancy ☐ Disability ☐ Mental health well-being ☐ Psychometrics	
Financial history	
☐ Financial history	

Biometrics	
BIOMETRICS ☐ Blood typing, ☐ Fingerprinting ☐ DNA analysis ☐ Retinal scanning ☐ Voice recognition ☐ Alco/blood concentration	
Personal opinions	
☐ Personal opinions, views or preferences of the Data Subject	
Views or opinions of another individual about the Data Subject	
☐ Views or opinions of another individual about the Data Subject	
Security access control **Biometrics** **Photographs and CCTV**	
☐ Photographs and CCTV footage if an individual can be identified by the footage	
Biometrics ☐ Blood type ☐ Fingerprinting ☐ Alco/blood concentration	
☐ Fingerprinting	

Children	
Information pertaining to children such as ☐ Name ☐ Next of kin ☐ Parents ☐ Address ☐ Telephone details ☐ Email ☐ School	

3. Duration of the Processing of Personal Data

The Processing of the Personal Information will be carried out over the periods set out below:

DURATION	

4. Location of Personal Data Processing

The Processing of the Personal Information will be carried out at the following locations:

LOCATIONS	

"None of the abovementioned Personal Data will be transferred outside SOUTH AFRICA.

5. Disclosure and other Operators or Data Processors to be used

Recipients

The Personal Information belonging to the abovementioned Data Subjects may only be disclosed to the following recipients or categories of recipients:

Sensitive Data (If Appropriate)

The personal data transferred concerns the following categories of sensitive data:

SUB PROCESSORS OR OPERATORS

The Processing of the Personal Information will be carried out by the Operator and the following Sub-Operators or Processors:

Name of Sub- Processor(s)	**Localization**	**Type of Processing**

Any modification to the above listing shall be agreed in writing between the Parties, through an Amendment to this Operator Agreement.

6. Maximum Duration of Personal Data Retention and Deletion Rules

The Operator will return the Personal Information to [COMPANY NAME] within 30 (thirty) days.

Where the Operator is not required to return the Personal Information to [COMPANY NAME], then the Operator will retain the Personal Information for a period of 3 years from the date of termination of the Agreement, and after such period it will delete the Personal Information as follows:

DELETION	

ANNEXURE B

ONWARDS TRANSMISSION NOTE

We, ……., the Operator acting on behalf of [COMPANY NAME], in response to your query and related request for certain Personal Information, identified below, have been given permission by [COMPANY NAME] to provide you with said information:

Details of requested Information of a Personal Nature

_____

_____

_____

Reason or Purpose why you require the information

_____

_____

_____

Permission from [COMPANY NAME] to send said information onwards

_____

_____

_____

Conditions and Terms attaching to onward transmission and subsequent processing of the requested Personal Information

- You will keep the information private and confidential;
- You may only use the information for the purpose described above and for no other purpose;
- You will safeguard the information;
- You will ensure that the information is kept safe and secure from unlawful or unauthorised access, and you will ensure that the integrity of the information is not compromised or altered in any manner;
- When using the information, you will comply with the processing conditions and provisions set out under a law known as the Protection of Personal Information Act, 4 of 2013, (POPIA),

and you agree to indemnify [COMPANY NAME], the Operator, and / or all and any third parties, including any affected Data Subject against all and any damages, expenses and / or costs and any legal claims and related costs and damages, which may be incurred or brought against by whomsoever as a result of your non-compliance with the above undertakings.

Furthermore, you acknowledge that [COMPANY NAME], the Operator, and / or all and any third parties, including third parties, including any affected Data Subject may institute legal action against you under the provisions housed under POPIA should you breach the abovementioned terms.

ANNEXURE C

SECURITY SERVICE LEVEL AGREEMENT

TECHNICAL AND OPERATIONS SECURITY MEASURES

Organizational Safeguards

The Operator must:

- provide [COMPANY NAME] with its information security policies, procedures and standards;
- using Information Security Officers and led by its Head of Information carry out annual security assessments in respect of the Personal Information which it is processing on behalf of [COMPANY NAME];
- limit and control the physical access to its buildings using effective access control mechanisms (for instance key cards);
- ensure that all entrances to its offices are staffed by receptionists and security staff and that effective access control procedures are in place;
- instruct and educate all employees on data protection and information security matters upon commencing employment and ensure that those who will be handling or processing the Personal Information identified under Annexure "A", are subject to and sign confidentiality obligations in respect of such information;
- implement a clear desk policy.

1. Information Security Policy

The Operator must document its Information Security Policies and follow Information Security programs that are based on at least one of the following frameworks:

- ISO 27001 & ISO 27002 standards
- NIST 800 Special Security Publications.

2. Information Security Framework

The Operator must define, document, and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards, and procedures.

The Operator must ensure that the assigned role is of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.

3. Asset Management

The Operator must design, document, implement and maintain an IT asset management process.

The Operator must document, implement, and maintain rules for the acceptable use of its assets and access management.

4. Human Resources Security

The Operator must:

- ensure all employees, contractors, and sub-contractors who access its IT assets and systems are screened prior to employment or contract;
- ensure that an Information Security awareness campaign is provided to everyone who has access to its IT assets. The Information Security campaign must educate personnel of their responsibility to secure the Operator's IT assets;
- ensure all user IDs, tokens or physical-access badges are assigned to a unique employee or subcontractor; and
- ensure all user/system/service/administrator accounts and passwords are never shared.

5. Physical and Environmental Security

The Operator must implement all appropriate information security controls to protect its IT assets from:

- Natural disasters;
- Theft, physical intrusion, unlawful and unauthorized physical access; and
- Ventilation, Heat or Cooling problems, power failures or outages.

6. Operations Management

Network Security: The Operator must ensure that Intrusion monitoring services are employed at perimeter points where the Operator's controlled confidential or Personal Information is used.

The Operator must ensure that all unnecessary services, ports, and network traffic are disabled.

System Security: The Operator must have a process for applying and managing security updates, patches, fixes upgrades, (collectively referred to as "Patches") on all systems.

The Operator must ensure that:

- patches that provide security fixes or security updates are tested and deployed within 45 -days from the date of release;
- all exceptions are documented, and it sets out and describes the reason for not deploying such Patches; and
- malware, Virus, Trojan and Spyware protection programs are deployed on all IT systems.

The Operator must ensure that all unused or unnecessary software, applications, services, sample / default files and folders are disabled on all IT systems.

7. Operation Security

The Operator must:

- ensure that any changes to IT systems that are performing work in respect of the [COMPANY NAME] information do not have any negative security implications.
- follow documented change management practices and procedures.

8. Disaster Recovery

The Operator must:

- implement appropriate disaster recovery measures to ensure that the Personal Information and Data it processes on behalf of [COMPANY NAME] can be re-instated in the event of loss or destruction of that data; and
- ensure that its disaster recovery plan defines RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives) of 24 hours for its Dimensions Online data collection platform.

9. Data Management

Data Security

The Operator must:

- use strong encryption key management practices to ensure the availability of encrypted authoritative information;
- encrypt all data assets in transmission between [COMPANY NAME] and the Operator as well as between the Operator and all other third-parties; and
- in the case that a public / private encryption tool is used, take every step to protect the private key.

Transferring of Data

The Operator must implement the following Acceptable Methods of Data Transfer:

- Secure File Transfer Protocol (sftp) – tcp port 22;
- host a sftp site for use by its Clients and vendors; and
- HTTPS – tcp port 443.

Handling of Data

Only the Operator's staff are permitted to handle and process the Personal Information which has been provided to it by [COMPANY NAME] under the Operator Agreement unless otherwise agreed in writing.

Storage of Data

The Operator must store the Personal Information which has been provided to it:

- on a server that is physically secured and is only accessed by authorized staff;
- on a server that is protected behind a firewall and that is properly patched with the latest Patches; and
- on backup tapes. The backup tapes are used for disaster recovery and are not retained. Tapes are overwritten after a set amount of time to a maximum of one year.

Data Destruction Process

Working storage media will either be wiped, shredded, stored or degaussed;

Non-working storage media will be shredded, stored degaussed as follows:

- Hard Disk and Media Storage
  - Functioning or non-function hard disks or electronic media such as tapes awaiting destruction by means of shredding, degaussing or wiping are stored in a secured location.

- Media Destruction Standards
  - Hard Drives will be disintegrated to a particle size no greater than ¼ inch or 0.635 cm;
  - CD's, DVD's, Backup tapes, audio cassettes, and video cassettes are shredded to ½ inch or 1.27 cm;
  - Paper documents will be shredded crosscut on site.

- Hard Disk Wipe Standards
  - All hard disks ready for destruction or disposal must be wiped using the DBAN utility;
  - Wipe Method of US DOD;
  - 7 passes;
  - Enable Verification.

Access Management of IT Systems

The Operator must ensure that:

- logical access controls are in place and restrict access to data on a need-to-know level;

- It uses authentication and authorization technologies for service, user and administrator level accounts;
- IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks are performed using non-administrator user accounts;
- Ensure password policies and standards exist on IT systems; and
- Ensure the following password requirements at all times:

    - Minimum length of 8 characters;
    - Complexity must contain at least three of the following four characters (Number, Uppercase Letter, Lowercase letter, Printable special character);
    - When changing or rotating an account password, the reuse of any of the prior 6 passwords is not allowed;
    - Account password expiration (the requirement to change and existing account password), must occur at - or less than 90 days;
    - Failed login attempts, when exceeding 3 consecutive attempts, must lock the account; and
    - Screen saver locks must be enabled to lock access latest after 30 minutes of user inactivity.

- The Operator must ensure that:

    - Authentication credentials are encrypted when stored or transmitted at all times;
    - It changes passwords immediately whenever it is believed that an account may have been compromised;
    - User's identities are verified before their password is reset and email or voicemail notification must be sent to notify the user that their password was reset;
    - User accounts are configured to force a change of their password upon first use of a new account or after a password is reset;
    - Password fields only display masked characters; and
    - All systems prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels.

- The Operator must ensure that procedures exist for prompt modification or termination of access or rights in response to organizational changes;
- The Operator must ensure that procedures exist for provisioning privileged accounts; and
- The Operator must ensure that it periodically reviews the necessity of privileged access accounts

10. Information Technology Acquisition and Maintenance

The Operator must ensure that infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices

11. Information Security Incident Management

The Operator must ensure:

- access and activity audit and logging procedures, including access attempts and privileged access, exist;
- logging includes all facility, application, server and network device and IDS/IPS logs are centrally managed and maintained for no less than 6 months; and
- security incident response planning and notification procedures exist to monitor, react, notify, investigate and mitigate or rectify incidents.