Data Access control record

| | |
|---|---|
| Purpose | The Data Access Control Record that I have chosen to develop is a centralised document that is utilised by individuals and management to track and manage access permissions across xy innovate system and servers. The reasoning behind is that we would be required by certain regulations such as GDPR and iso27001 frameworks to ensure that there is level of accountability and adherence to these frameworks when we are reviewing access management. |
| Scope | The scope in this context would be that this record is applicable and relevant to all the systems that handle sensitive data which would include the digital ocean wallet service, the HR records, and customer data bases and server that are stored in our physical location. This would be applicable to all individuals, third party individual and contractors that would require access to our sensitive information. |
| Record Details | This record has been specifically developed to ensure that it contains an extremely comprehensive log of access and approvals. The key policy in place here is the rule of least access for individuals to maintain our security.<br><br>1) Asset name – this is the system or assets that we are utilising and working with at the current time for example customer financial data databases.<br><br>2) User Role- This would refer to the role and level of authority of an individual attempting to access the data records. This may be the manager or a supervisor or an auditor etc. This could refer to any role associated with the organisation (internally or externally)<br><br>3) Access level- this would be in the form of access either granted and if this would be partial or full access i.e. read only / edit access for the relevant data and documents at hand.<br><br>4) Justifications- The justification as to why this access would be granted or denied would be based on the role of the individual and the reasoning behind why this would be required to grant access for example due to legal compliance or part of a company project where access to data would be required<br><br>5) Approval Authority – This would be the individual who would sign off on the approval of access to an individual requesting this. This authority would be the senior management or the digital wallet service manager. |

| | |
|---|---|
| | 6) Access expiry date- This is crucial to monitor and implement. A review should take place to ensure individuals are not granted access for longer than what would be required to complete the task at hand.<br><br>7) Monitoring Logs – this process would be key to review as reviewing seim data and access logs will help us to identify users and track their activities to ensure we are effectively monitoring individuals with access to critical information. |
| Maintenance protocol | The maintenance protocol is especially important because access requests are usually reviewed and monitored by the individual's direct manager which are then approved by the ciso, or the organisations equivalent to ensure that all the permissions that have been granted are appropriate. A quarterly review will then be conducted to review the access rights on a more technical and deeper level to ensure that the correct access companywide is appropriate and if any changes need to be made.<br><br>If any anomalies or unauthorised access is detected in these reviews, then they will be escalated immediately for investigation. This process is in direct alignment with the iso/IEC 27001 clause 5.2 (ISEO Blue, 2025) which highlights the importance of regular access reviews to keep access log controls up to date. |

**ISEO Blue, 2025.** ISO 27001 Control 5.2 – Policies for Information Security. *ISEO Blue*. Available at: https://www.iseoblue.com/post/iso-27001-control-5-2-policies-for-information-security#:~:text=This%20control%20ensures%20that%20a%20comprehensive%20set%20of,clear%20guidance%20and%20management%20commitment%20to%20safeguarding%20information. [Accessed 2 January 2025].