Remote access Policy

Policy Summary -	The Remote access policy ensures that there is a process to establish security measures to mitigate the security concerns and vulnerabilities that may come with remote working for employees while at the same time ensuring a level of organisational flexibility. This policy is in direct correlation with control 6.7 of the iso27001 (ISMS.online, 2025) standards as it outlines the importance of having a remote access policy alongside other regulations such as the ISO/IEC 27002 policy and GDPR standards
Introduction-	Introduction – A workforce and market shift to having more assets and individuals including a work from home model in the organization is crucial for us to understand and how organisations such as XY innovate could best prepare the organisation to face new challenges and issues while catering for remote access. This policy has been designed to provide a guideline on how to secure remote access and the ways that we are able to address risks such as authorized access, data breaches and compromised systems. This allows us to have a sense of employee accountability and responsibility when access and utilising systems remotely.
ISMS Scope-	This policy would apply to all the remote access categories highlighted below • This would apply to all the employees that would need to access information outside of the office this would usually be the software developers and database developers • This policy would apply to the contractors and external vendors alongside third-party individuals that would require temporary or sustained access to carry out an important role in developing or maintaining the security of our data. • This policy would also apply not only to individuals but to devices and systems such as the digital wallet platform databases that would be hosted on digital oceans cloud platforms. • This policy would have an exclusion, this would be systems that we have identified via our risk assessment to be too sensitive and critical for remote access such as the backend financial management system the encryption key management systems used for protecting the integrity of our data.
ISMS Objectives	The Objectives are to implement systems to mitigate the risks associated with remote working but implementing a secure encryption method in place. It is also to ensure that all information is stored, trades or released by the organisation is of absolute integrity. Another Key objective is to ensure the compliance of the ISO/IEC 27001 and GDPR requirements this objective ensures that all the information is stored and maintained in accordance with clear guidelines which ensure a sense of accountability and overall organisational system security during remote access of assets. Another key objective would be to ensure a sense of flexibility while

	maintaining our security practices to not make the organisation a large group of stringent policies which may impact workflow and productivity.
ISMS Remote access Principles	1) The first policy I will introduce is that of implementing a Multi Factor authentication (MFA) for all remote employees and external 3rd part individuals for digital ocean this may be a shared cloud environment where employees would be required to log into our systems with the correct credentials and they be able to access critical data. 2) RBAC would be essential for this policy. This would be when data and information is only provided to individuals with the correct level of authority and specific role such as the software developer would have access however a network technician would not. 3) A secure layer of communication across the organization must be in place. Especially if remote work is to be implemented or manged effectively. VPN'S must be in use with the relevant encryption protocols such as SSL/TLS. Another key point to address would be that access to the digital wallet Api would be restricted to whitelisted IP address to allow for an increased layer of security. 4) Device management – the devices that would be used would need to ensure they are compliant with the correct level of security such as anti-malware 5) Employee accountability- This is crucial as Employees are also accountable for ensuring that the objectives for the isms are established and correctly implemented via employees' actions. They must adhere to stringent guidelines to avoid any practices that may misalign with the policies that the organisation is aiming to implement. The responsibility that employees have is not only limited to their usage of the systems however their response to breaches and issues. Employees must report any security incidents or breaches to the incident response team / management.
Responsibilities	The implementation of this policy is carefully constructed so that we utilise the joint efforts and resources of all the stakeholders that would be involved in xy innovate to ensure the effectiveness of new policies and procedure. The controls what I have identified that need to be implemented are varied and cover different aspects of the organization. The control would include the VPN infrastructure alongside monitoring access logs and ensuring a level of compliance with technical security measures. The employees in the organisation must ensure that they are following the security measures and using authorized and secure devices alongside ensuring that incidents are reported accurately. The management across the digital wallet team, IT team and the administration team are responsible for ensuring that the implementation procedures for the isms are correctly established and finalised this would be done via regular meetings and discussion. Audits are conducted to explore what would need to be implemented in the organisation for example access rights privileges may have not been updated recently and this would be a point of concerns alongside the resources that would need to be utilised to implement the policy would be required for a certain issue such as Remote access policy or advanced malware system. The main point of day-to-day authority surrounding the organisation management would be the

	digital wallet software manager and this person would be responsible for addressing anything to do with the digital wallet service.
Challenges and exclusions	Remote access has its own challenges and issues related to security. Certain assets have been excluded from the remote access policy due to the nature and sensitivity of these assets for example the back end financial systems and the encryption management system for the integrity of data. Employees that do not have the relevant access levels have also been restricted from remote working due to GDPR and compliance reasons. Another key issue would be the strength of the network connectivity at home and outside of the office which would pose further issues.
Expected Outcome	The experienced outcome is that this policy would improve the security and risk of remote working by impending controls and policies to help with breaches and unauthorized access via access controls. This would also ensure compliance with the ISO 27001 and GDPR regulations by ensuring an increased level of stakeholder trust in our organisation by improving xy innovates working arguments this would directly improve the company employee retention issue and overall levels of happiness and job satisfaction which would lead to increased motivation and productivity. This policy would also lead to a development of a culture that promotes accountability and security awareness which enforces xy innovates capacity to response to ever growing threats and issues.

ISMS.online, 2025. ISO 27001 Annex A.6.7 Remote Working 2022. *ISMS.online*. Available at: https://www.isms.online/iso-27001/annex-a/6-7-remote-working-2022/ [Accessed 2 January 2025].