12/8/2024

BW-P2403

Security Policy

This policy applies to all Black Wolf employees.

Its purpose is to foster a positive corporate culture and promote proactive security practices. Since security threats are dynamic, they can impact all areas of the company, and therefore, security must be integrated into all activities.

1. Manual documentation and reporting are prohibited. Financial reports must be generated only through SAP Business One, and other departmental reports must be proof-based (e.g:. Incident Reports).
2. Employees must protect company assets, maintain confidentiality of sensitive information, and report any security breaches promptly to their line managers.
3. Security considerations must be integrated into all actions and daily activities, regardless of the employee's position within the company hierarchy.
4. Regular security awareness programs will be conducted to educate staff about potential risks and promote a secure environment.
5. Employees are accountable for the security of information they access. Sensitive information must only be accessed when necessary for their roles, and any access must be monitored by relevant line managers.
6. Employees must not access or interfere with sensitive information outside the scope of their assigned duties. This includes financial documents, proprietary data, and any confidential materials.
7. Any employee found accessing or disclosing sensitive information without proper authorization will face disciplinary action, which may include termination of employment.
8. Employees must act ethically in all work-related activities and handle confidential information, as well as the rights and opinions of colleagues and stakeholders, with professionalism and respect.
9. All credentials and data related to company software must be kept confidential. Staff members are prohibited from interfering with colleagues' software processes or activities.

Yad Mohammed Rashid

General Manager