NO.
1
2
3
4
5

IDENTIFIABLE RISK
Velo Compute has not established an appropriate document, guide or framework to truly manage security information, general security policies and topic-specific security policies. Common security practices, such as passwords length, are just assumed by all personnel to be correct.
Velo Compute does not presents appropriate communication channels within the company. All communication is done through WhatsApp groups, emails and Microsoft Teams Platform. Moreover, communication with law regulatory bodies is performed the same way. Confidential information such as code fragments of the VeloAnalytics SaaS Platform is shared through screenshots.
Velo Compute does not have an individual or department designated to attend cybersecurity risks, or any identified threat that could damage business continuity. In fact, when a threat is detected the whole business operation are stopped. The CEO is then informed by the personnel who detected a possible threat, and together, make a decision. There is no history of fixes storaged or procedures to stop common threats, mainly because their operations run on the cloud. But even if this is expected, in the future the company may expand and could purchase on-premise servers for specific storage of data, making threat intelligence a must-
Three Departments have access to Personally Identifiable Information (PII): Engineering, Data Science and Sales (to some extent). Engineering, through their operations in their AWS platform can usually access to the clients purchases and data, including phone number, full name. Data Science, while they perform data depuration can see previous clients data too. This wouldn't be so alarming if we consider both departments need the data to perform their activities in a daily basis. But, remote culture in the company becomes a risk for PII privacy and Integrity. In fact, the company does not demand their employees to use any type of authentication besides of their usernames and passwords. Condiring that personnel laptops could go missing in their homes or some other member of their families could access clients data just by knowing the username and password is a significant risk.
With termination of a contract, personnel must return their work laptops to HR Department, then their credentials are removed. Some of Velo Compute past employees have accessed their work account months after termination of their contract. New employees have been asked that upon detection of external log ins, please contact HR department in order to correct and eliminate credentials. These kinds of incidents indicate that HR department is not managing the deletion of past employees credentials swiftly. Furthermore, it seems that ocassionally, that department forgets to erase some of those credentials.

RISKS

Velo Compute will treat **RISK #1** by implementing controls:

Velo Compute will treat **RISK #2** by implementing controls:

Velo Compute will treat **RISK #3** by implementing controls:

Velo Compute will treat **RISK #4** by implementing controls:

Velo Compute will treat **RISK #5** by implementing controls:

RISK ASSESMENT

RISK OWNER	IMPACT	IMPACT SCORE (1-5)
Top Management (Velo Compute CEO)	No Foundation to establish security policies, or information security policies and practices. Unable to stablish an Information Security Management System (ISMS).	5
Top Management (Velo Compute CEO)	Information security policies and topic-specific policies cannot be commuicated within personnel in an appropiate way, decreasing awareness both from personnel and from interested parties. Risk behavior is common and can provoke information leak. Intellectual property at risk. Moreover, a defined channel for communicating with law regulatory bodies needs to be established.	3
Top management (Velo Compute CEO)	Not having a designated individual or group within the organization that can identify threats, cybersecurity incidents and respond to them accordingly to their capabilities is counterproductive, specially if we consider that the entire business operations must stop to find a solution to a threat.	4
Top Management (Velo Compute CEO) -> Engineering Department/Data Science Department	Data exfiltration, loss of clients trust. Loss of unencrypted assets are some of the worst scenarios that these behaviors present.	4
HR Department	PII privacy and integrity is constantly at risk. Remote log in of past workers with malicious intent can damage the company reputation, endanger clients data integrity.	4

RISK TREATMENT

Annex A Controls

5.1 Policies for Information Security (Organizational Controls)
5.4 Management Responsabilities (Organizational Controls)
5.23 Information Security for use of cloud services (Organizational Controls)
6.3 Information Security Awareness, Education and Training (People Controls)

5.4 Management Responsabilities (Organizational Controls)
5.34 Privacy and protection of PII (Organizational Controls)
6.3 Information Security Awareness, Education and Training (People Controls)
6.7 Remote Working (People Controls)

5.7 Threat Intelligence (Organizational Controls)
5.34 Privacy and protection of PII (Organizational Controls)
8.7 Protection against malware (Organizational Controls)

5.34 Privacy and protection of PII (Organizational Controls)
8.4 Access to source code (Technological Controls)
8.5 Secure Authentication (Technological Controls)
5.18 Access Rights (Organizational Controls)
8.11 Data Masking (Technological Controls)
8.7 Protection against malware (Technological Controls)
6.3 Information Security Awareness, Education and Training (People Controls)

5.18 Access Rights (Organizational Controls)
8.10 Information deletion (Technological Controls)
5.11 Return of Assets (Organizational Controls)

Annex A Control Group Identified
Organizational Controls/People Controls/Technological Controls
Organizational Controls/People Controls
Organizational Controls
Organizational Controls/Technological Controls
Technological Control/ People Control/ Organizational Control

VELOCOMPU

RISK IMPACT	
Insignificant	1
Minor	2
Moderate	3

Major	4
Catastrophic	5

TE