	Control Group	Ref.
	Organizational Controls	5.1
	Organizational Controls	5.4
	Organizational Controls	5.7
	Organizational Controls	5.18
	Organizational Controls	5.23
	Organizational Controls	5.34
	Organizational Controls	5.11

	People Controls	6.3
	People Controls	6.7
	Technological Controls	8.4
	Technological Controls	8.5
	Technological Controls	8.7
	Technological Controls	8.10
	Technological Controls	8.11

Name
Policies for Information Security
Management Responsabilities
Threat Intelligence
Access rights
Information security for use of cloud services
Privacy and protection of PII
Return of assets

Information security awareness, education and training
Remote Working
Access to source code
Secure Authentication
Protection against malware
Information deletion
Data masking

Control
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the Organization.
Information relating to information security threats should be collected and analysed to produce threat intelligence.
Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the Organization's topic-specific policy on and rules for access control.
Processes for acquisition, use, management and exit from cloud services should be established in accordance with the Organization's information security requirements
The Organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
Personnel and other interested parties as appropriate should return all the Organization's assets in their possession upon change or termination of their employment, contract or agreement.

Personnel of the Organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the Organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the Organization’s premises.
Read and write access to source code, development tools and software libraries should be appropriately managed.
Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.
Protection against malware should be implemented and supported by appropriate user awareness.
Information stored in information systems, devices or in any other storage media should be deleted when no longer required.
Data masking should be used in accordance with the Organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Applicable	Justification for Exclusion
YES	
YES	
YES	
YES	
YES	
YES	
YES	

YES	
YES	
YES	
YES	
YES	
YES	
YES	

Implementation Status
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED

IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED
IMPLEMENTED

Comments
Foundation for further policy creation. Ensures that information security policy is correctly communicated and approved by the top management. Moreover,states that security policy and topic-specific policies must be reviewed at planned intervals, and alligned with the interested parties interests.
This Control ensures that all personnel is aware of the information security policy. Considering Velo Compute startup status and remote-work culture, employees need to be strictly aware of these kinds of policies.
Considering that Velo Compute is a startup with a very demanding business model (Predictive analysis using AI models), the company must carefully analize every threat collected to produce ways to protect their business.
Personally Identifiable Information (PII) must be confidential for not authorized personnel. Needs to maintain its integrity after its depuration process in the Department of Data Science.
Velo Compute utilizes web services (AWS) to run their VeloAnalytics Saas Platform. It is indispensable that the activity in the cloud is aligned with security requirements.
Velo Compute manages a high input of PII from EU/US customers. Their business integrity and success is based on maintaining the integrity, authenticity and confidentiality of PII in order to maintain their predictive AI models.
The Department of HR and Operations manage the purchase of laptops for employees to work remotely from various El Salvador locations. Implementing Annex A 5.11 ensures that upon termination of contract or abandonment of company, employees must return assets (laptops).

Startups definitely need to start as soon as possible educating their employees on information security awareness. It's a plus when starting business and adds credibility to the company.
Fundamental when working 100% remotely. Remote work indeed adds flexibility to work environments, but it also needs to be regulated.
Intellectual property (AI predictive models) source code must be managed only by allowed employees to maintain its integrity and confidentiality. Moreover, the development tools and cloud environment used must receive the same treatment to ensure no malfuctions or errors by unauthorized employees.
This control projects secure authentication as a pilar for information security. PII must be secure in every employee endpoint, specially considering a remote work culture. The company could invest in a multi-factor authentication process, such as YubiKey.
Protection such as antivirus software, web filtering and anti-ransomware are most of the time the frontlines of a startup security environment.
Combined with 5.11, ensures that no PII data is storaged on laptops that are no longer being used.
Indispensable for secure development lifecycle. Tools like encryption or substitution used to secure the storage and processing of PII.