

Information Security Policy

Content Table

- [1.0 Purpose](#)
- [2.0 Scope](#)
- [2.1 Audience](#)
- [2.2 Applicability](#)
- [2.3 Glossary](#)
- [3.0 Objectives](#)
- [4.0 Responsibilities](#)
- [5.0 Policy Statement](#)
- [5.1 Data Classification](#)
- [5.2 Information Access Control](#)
- [5.2.1 Network and System Access](#)
- [5.2.2 User Account and Password Management](#)
- [5.3 Acceptable Use](#)
- [5.4 Internet Access](#)
- [5.5 Email and Communication Tools](#)
- [5.6 Social Media and Blogging](#)
- [5.7 Clear Desk and Clear Screen Policy](#)
- [5.8 Remote Working Security Controls](#)
- [5.9 Personal Use of Devices](#)
- [5.10 Equipment / Data Disposal](#)
- [5.11 Reporting Information Security Incidents](#)
- [5.12 Compliance](#)
- [6.0 Policy Exception](#)
- [7.0 Document Management](#)
- [7.1 Validity and Document Management](#)
- [8.0 References](#)

1.0 Purpose

Global Software Solutions NV (the ‘Company’) is critically dependent on Information and information systems. If important Information is disclosed to inappropriate persons or misused, the Company could suffer serious losses and claims, including reputation loss.

2.0 Scope

2.1 Audience

This Policy applies to all employees, consultants and contractors of the Company.

2.2 Applicability

The policy requirements apply to all computer, smartphones, network systems and services (including systems hosted on the Cloud) owned or administered by the Company.

2.3 Glossary

Availability - The quality of being able to be used or obtained.

Confidentiality - The state of keeping or being kept secret or private.

Cloud - It is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. This service is designed to either store and manage data, and run applications.

Guest - A guest is a visitor such as a vendor, supplier, contractor, or any other person with whom the Company has a commercial (or prospective) relationship. Guests having no commercial relationship with the Company should be approved by senior management prior to accessing the Company offices.

Information - is data that contains valuable records for the Company. It can be a database, a document or any type of data which can be related to financial records, personnel data, system documentation, etc. related to the Company.

Integrity - Internal consistency, accuracy and/or lack of corruption of data in whichever format.

Users - Employees, consultants or contractors employed by the Company.

3.0 Objectives

The objective of this policy is to provide guidance to all Users about information security requirements and principles to adopt to secure Confidentiality, Integrity and Availability of Information used by the Company.

4.0 Responsibilities

All Users who have access to the Company's technology resources (e.g. IT systems) and information are responsible for:

- Knowing and understanding the policies that apply to the Company's technology resources and information in use;
- Exercising good judgment in adherence to the principles of this policy especially when accessing the Company technology resources and information;
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of the Company Information.

5.0 Policy Statement

5.1 Data Classification

It is the responsibility of all Users to classify documents Secret, Confidential, Internal Use or Public accordance to the Information Classification. For examples refer to the table below.

Classification Level	Description	Examples
----------------------	-------------	----------

Secret	Information that is considered highly sensitive that requires special authorization for use and collection.	• PII data e.g. employee and customer information • Passwords
Confidential	Day-to-day business Information of high sensitivity. More considerations need to be made around protecting and disseminating this Information, as it could expose the Company to unnecessary risk if improperly handled.	• Technical design and architecture documentation • Software source code
Internal Use	Technical design and architecture documentation Software source code	• Organization charts • Policies and procedures • Email correspondence • Financial records
Public	Information that can be disclosed without restriction or is expected to be known publicly	• Published marketing materials • Published financial reports

5.2 Information Access Control

5.2.1 Network and System Access

- Access to Company's Information will be provided based on the need-to-know basis. Information can be disclosed only to people who have a legitimate business need for the Information. Disclosure of sensitive, confidential, restricted or internal information for new relationships e.g. with new suppliers, IT vendors, require a Non-Disclosure Agreement, NDA which is agreed by respective Head of Legal.
- Access to all systems, services and Information is forbidden, unless expressly permitted to individual users or groups of users. A user registration process for employees is adopted to grant access to the Company systems and Information by making a request to IT Helpdesk by raising a Jira Ticket.

- System utilities (programs, files, or functions) that are capable of overriding system and application controls shall be restricted and authorised to be used by dedicated teams. Examples of Privileged Utility Programs include, but are not limited to, account management, backup utilities, and other.

5.2.2 User Account and Password Management

- Users must use a unique user IDs issued by the Company and private password. Passwords must be at least 12 character long, containing one numbers, one symbols, one normal and capital letter. Password must be changed every 90 days and a minimum password change to 3 days. Used password count is 20 where user cannot use last 20 passwords used previously. This request applicability depends if support by the infrastructure and application.
- Users must be responsible for the use and safeguarding of their user IDs and passwords. The password is personal and it is forbidden to pass it on to another person, such as to family members, friends, colleagues, etc. This would include not letting other persons using the Company equipment provided, such as the laptop. Temporary unique passwords are provided to Users from IT Helpdesk team for a new IT service and password reset request, where Users must change their passwords during the first attempt to login to an IT asset or system.
- Users will be required to adopt Microsoft Single Sign-on and Multi-factor authentication for on-cloud services, e.g. Atlassian Jira and Confluence, and others adopted in future.
- Passwords must not be stored in readable form example, written on a paper, in batch files, scripts, software macros, terminal function keys and other formats.
- Users must lock their terminal or log off when leaving their computer unattended, to prevent unauthorised users accessing the system in your absence.

5.3 Acceptable Use

- Company's Information stored on whatever media on computing devices or on-cloud remains the property of the Company at all times.
- Storing of confidential or sensitive Information on removable media (e.g. USB memory sticks, external USB hard disks) is prohibited unless an exception is approved by Information Security.
- Introduction of malicious programs into the network or server infrastructure is prohibited.
- Affecting security breaches or disruptions of network communication is strictly prohibited. Security breaches include, but are not limited to, accessing data of which the User is not an intended user or recipient.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet, is strictly prohibited.
- Users are responsible for the physical security of any computer or any other device provided by the Company, which includes mobiles, tablets, and others assets. If device is damaged due to carelessness, the User is liable to pay for any damages or the cost of replacement.
- Providing Information about or lists of the Company employees or expose sensitive information (e.g. player database) to parties outside the Company is strictly prohibited unless there is a specific reason, e.g. payroll services.

5.4 Internet Access

- Users are provided with Internet access to perform their job duties. They must not view or download offensive, illegal, and discriminatory content.
- Users must take special care to ensure that they do not represent the Company on Internet discussion groups and in other public forums, unless they have been authorised to do so as part of their role and/or the job description.
- Sensitive and confidential Information, including passwords must not be sent across the Internet unless this Information is in encrypted form, e.g. sharing password using Password Manager software, provided by the Company.
- Unauthorized copying of copyrighted material including digitization and the installation of any copyrighted software is strictly prohibited.

5.5 Email and Communication Tools

- Users will be granted access to email through creation of an unique account (user ID) and access to data and information according to need to know basis.
- Users must use extreme caution when opening email attachments received from unknown senders, which may contain malware. For example, Users must not open an email coming from an unknown sender. This email should be reported to IT Helpdesk through Slack or open a Jira ticket.
- The following activities are strictly prohibited:
 - a) Sending unsolicited email messages on behalf of the Company, including the sending of "junk mail" or other advertising material to individuals,
 - b) Unauthorized use, or forging, of email header Information.
 - c) Creating or forwarding chain letters,
 - d) Posting the same or similar non-business-related messages to large numbers of users,
 - e) Sending sensitive Information, example passwords, or others,

- f) Sharing sensitive or confidential data with individuals within or outside the Company using a communication tool such as Slack should be limited unless it is authorised by the management. e.g. sharing a document containing any personal identifiable information using Slack. This should be shared by using Microsoft OneDrive or any other Company tool as may be provided by the Company, since OneDrive enforces authentication, encryption and user permissions controls,
- g) Other communication tools such as; WhatsApp, Skype personal and others are prohibited to be used to communicate with employees and third parties on work related matters, except if the WhatsApp and Skype account in use is created on the Company behalf. The Company official communication tool to be used is Slack and Teams.

5.6 Social Media and Blogging

- The following activities are strictly prohibited to reduce the risk of unauthorised disclosure of or access to the Company Information:
 - a) Extensive blogging by Users unless authorized by the Company (such as for HR and Marketing employees) is prohibited whether using the Company property or personal computer systems. Limited and occasional use of the Company IT systems resources to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, is not detrimental to the Company interests.
 - b) Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Company and/or any of its employees.

5.7 Clear Desk and Clear Screen Policy

- In order to reduce the risk of unauthorised access or loss of information, the Company enforces a clear desk and screen policy as follows:
 - a) All computing devices are secured with a password protected screensaver with the automatic activation. Users must lock the screen or log off when the device is unattended.
 - b) Following meetings at any of the Company's meeting rooms, sensitive Information written or drawn on whiteboards must be erased.
 - c) Care must be taken to not leave confidential or sensitive printable material on printers, photocopiers desk, meeting rooms, etc.
 - d) All business-related printed matter must be disposed securely (e.g. using shredders / confidential bins).

5.8 Remote Working Security Controls

- Remote users include all Users not located at the Company's premises. Users will be granted access to Company's data and IT systems by connecting with a VPN software or any such other connection method or tool as may be provided by the Company from time to time.
- Users must ensure that while remote working, except when working from home, must connect to the internet using the VPN software. Whilst remote working, using the browser to access Company's services for e.g. Email, Jira or any other supported web based format is permitted. Setting the browser to use private mode functionality is to be used, e.g. use Incognito mode in Chrome browser.
- Always ensure that your corporate devices are safely stored away if unattended. You should apply a common-sense approach to storing your laptop.
- Whilst traveling, especially in public spaces such as airports, you should ensure that your corporate device is in your possession at all times, and you should ensure that your screen is not visible to others when viewing any confidential and / or sensitive material.
- If traveling by car with your laptop, always ensure that your laptop is stored out of view of potential thieves (e.g. under the seat or in the boot of the vehicle) whether you are in the car or not. Where possible, do not leave your laptop in your vehicle whilst unattended.
- Report immediate loss or theft of Company's equipment, e.g. a laptop to the IT Helpdesk by message IT Helpdesk in Slack. Also, a police report should be provided as an evidence in case of theft of the Company's equipment.

5.9 Personal Use of Devices

- A reasonable personal use of the Company devices is permitted. However, it must not be in any way detrimental to the user's own or their colleagues' productivity, nor should it result in any direct cost to the Company.
- The Company reserves the right to audit and monitor network, IT systems, telephone, e-mail, voicemail, internet and other communications. This may include examination of the content stored within the Company email and data files of any user.
- For business reasons, and in order to carry out legal obligations as an employer, your use of our systems including the telephone and computer systems may be continually monitored by automated software or otherwise, and at all times as permitted by applicable law. We provide the tools and equipment for business use and reserve the right to retrieve the contents of e-mail messages or check internet usage as reasonably necessary in the interests of the business and as permitted by law, including for the following purposes (this list is not exhaustive):

- a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
- b) to find lost messages or to retrieve messages lost due to computer failure;
- c) to assist in the investigation of alleged wrongdoing;
- d) to establish, exercise or defend legal claims and to comply with any legal obligation.

5.10 Equipment / Data Disposal

When sensitive information is erased from a disk, tape, or other reusable data storage media, it must be followed by a repeated overwrite operation in order to obliterate the sensitive information.

Before any computer storage media is sent to a vendor for servicing, or disposal, all Company sensitive information must be destroyed. Hard disks must not be sent to vendors for equipment servicing.

The disposal of all paper documents that contain payment information such as bank account numbers or credit card numbers, must involve shredding or other approved destruction methods.

5.11 Reporting Information Security Incidents

A security incident and/or breached of this Policy must be reported. Examples of security incidents are infection by viruses or malicious software, theft or loss or unauthorized access to computer equipment, unauthorized or accidental access and/or disclosure of customer data, and others.

5.12 Compliance

- The Company will not tolerate any misuse of its systems and any suspected or actual violations of this Policy. Any inappropriate use of the Company equipment, technology,

internet, email, systems and tools and other resources or excessive personal use of the same may result in disciplinary action or may lead to termination of employment or contract, including immediately without notice, as permitted by law. In some circumstances illegal activity may warrant possible referral for the law enforcement authorities.

- All Users of the Company must comply with the requirements established by this Policy. All exceptions to the requirements must be requested to the Information Security Team.

6.0 Policy Exception

- Exception to the policy are deemed to be a business risk and hence need to be formally raised using the Policy Exception procedure, reviewed and approved by the **Line manager & C level**
- Exceptions shall be time limited and in the exception request there shall be a plan for how and when to comply
- Exceptions will be handled on a case-by-case basis, and no exception is to serve as a precedent to approving similar requests in the future
- Violations of the company information security policies and procedures, as well as information security *breaches** committed by employees or contractors shall be reported to a line manager, as soon as possible and may result in disciplinary action, leading up to and including dismissal (according to the Disciplinary Policy found on the HR Portal) - depending on certain factors such as the nature and gravity of its impact on the business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

**An information security breach is defined as the loss of confidentiality, integrity, availability and repudiation of information, exposing sensitive company information to unauthorized access, use, disclosure and/or modification.*

7.0 Document Management

7.1 Validity and Document Management

This policy applies to Global Software Solutions NV

