DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Purpose

The purpose of this document is to provide guidance on acceptable use of the business tools JIRA, Confluence, Bitbucket, Bamboo and Sonar (collectively "DOJO Atlassian Tools") for storing and sharing information for business purposes.

Applicability

These guidelines apply to all employees, temporary workers, interns, and other workers at Publicis Groupe, its agencies, brands, business units and shared service centers, and authorized third parties (freelancers, contractors, consultants, suppliers, etc.) collectively called 'People' in this document.
Publicis Groupe and its agencies (including brands, business units and shared service centers) are collectively called 'Groupe' in this document.

Introduction

DOJO Atlassian Tools is an on-premise Data Center service that enables People to securely collaborate on projects and software development from anywhere and on supported devices. DOJO Atlassian Tools can be used to share content with internal and external teams. DOJO Atlassian Tools comprise of:

- JIRA: a project management application enabling teams to plan and track project work, defects, issues, etc.
- Confluence: a wiki project teams can use to manage requirements, track decisions to closure, create how-to guides, capture meeting notes, &c.
- Bitbucket: a software source code management server based on the popular open-source Git distributed version control technology
- Bamboo: a continuous integration (CI) and software deployment tool that ties automated builds, tests, and releases together in a single workflow
- Sonar: provides continuous inspection of code quality, automatic reviews with static analysis, code coverage

Acknowledgement

DOJO Atlassian Tools are for business use only. Private use of these tools is not allowed. By using DOJO Atlassian Tools, People acknowledge full acceptance of the terms of guidelines. These guidelines enter into force as soon as People log into the tools.

If the terms of these guidelines are inconsistent or in conflict with the terms contained in Janus, or posted on the DOJO Atlassian Tools portal, the terms contained in this document shall prevail, to the exception of Janus Policy and the Acceptable Use Policy published by the Global Security Office, which shall always supersede over these guidelines.

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Monitoring

Any content uploaded on DOJO Atlassian Tools is monitored. Publicis Groupe reserves the right to investigate any violation of these guidelines or misuse of the DOJO Atlassian Tools and may suspend or remove any content that violates these guidelines or any other Publicis Groupe Policies.

Guidelines

Please refer to the following table for guidance on acceptable use of DOJO Atlassian Tools. If you have any questions or need further clarification, please contact the Global Security Office at askgso@publicisgroupe.com.

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Information Type	Allowed on DOJO Atlassian Tools
Public Information (i.e. information in the public domain) Definition: Non-sensitive. No anticipated disclosure harm. Includes, but is not limited to the following: a. News articles, office addresses, etc. b. Content shared with industry (e.g. award nominations, industry working groups, etc.)	Yes
Restricted Information Definition: Sensitive. Unauthorized disclosure may very likely cause some commercial, legal or branding damage to the Groupe. Includes, but is not limited to the following: a. Information for internal sharing, storage and collaboration such as company policies, project wins, all agreements (clients, suppliers, freelancers, etc.), project plans, client deliverables, insurance policies, etc. b. Information for external sharing, storage and collaboration driven by business needs e.g. Groupe's business contacts' information, documents for collaboration with clients, suppliers, industry partners, etc. c. Groupe or Client Personal Information such as email IDs, address, telephone numbers, etc.	Yes
Highly Restricted Information Definition: Highly sensitive. Unauthorized disclosure will cause serious commercial, legal or branding damage to Groupe. Includes, but is not limited to the following: a. Groupe or Client Sensitive Personal Information such as Credit Card Numbers, Passport Information, US SSN, Driver's License Numbers, Tax IDs, Insurance Numbers, Health Information that could be linked to an individual, etc. b. Groupe Intellectual Property such as unpublished patents, unpublished copyrighted materials, trade secrets, pricing models, business plans, undeclared financial results, etc. c. Any other confidential information with perceived high disclosure risks such as payroll information, financial information, network architecture diagram, performance reviews/succession planning or other confidential HR processes etc.	No
Non-business Information Includes, but is not limited to the following: personal music, personal movies, personal photos, personal materials, etc.	No

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Information Type	Allowed on DOJO Atlassian Tools
Harmful content Includes, but is not limited to, the content that: a. Violates any Groupe policies, including Janus and security policies. b. Communicates any message or material that is illegal or tortious, defamatory, harassing, libelous, threatening, or obscene. c. Knowingly violates or knowingly infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity. d. May otherwise be unlawful or gives rise to civil or criminal liability. e. In any manner that is likely to damage, disable, overburden, or impair the Box service or interfere in any way with the use or enjoyment of the Box service by others. f. Knowingly introduces any malware or other malicious activity in the use of the Box service. g. Violates any country denied party-list, embargoed country restriction, export law or regulation.	No
General Guidance	
Client information a. If your Client prohibits the use of cloud solutions for their engagement, contact the Global Security Office for guidance / options, and do not use DOJO Atlassian Tools until authorized by Client in writing. b. If your Client has a specific question about DOJO Atlassian Tools security, please contact the Global Security Office.	

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Information Type	Allowed on DOJO Atlassian Tools
Collaboration a. DOJO Atlassian Tools allows you to grant access to others if you are a project, space, or repository administrator. Use your best judgment and discretion while deciding the right level of access for others, especially external collaborators. b. Personal use of DOJO Atlassian Tools is not permitted. People shall not make personal copy of client data available on the Tools. c. Client material shall not be uploaded on any public facing website. Where prohibited, client data shall not be kept on DOJO Atlassian Tools for a period longer than permitted by client. d. People shall notify the loss of information, unauthorized access or compromise of information security controls immediately as a security incident to Global Security Office. e. People shall not intentionally destroy or alter any software source code or aid others to do so. f. DOJO Atlassian Tools allows you to share links to folders and files with others. Share only with people who are authorized to access that information or have a need to know. g. Always ensure that use of DOJO Atlassian Tools in providing our services to our clients does not violate any contractual agreements with them (e.g. use of cloud based systems or tools for providing our services). h. Please review regularly the list of People to ensure only authorized People have access to the Tools. Please ensure to remove People immediately when they leave the company, change roles or their contract ends.	
DOJO Atlassian Tools alternatives a. Use authorized internal systems for storing and internal sharing of information that is not allowed on DOJO Atlassian Tools. Examples of such systems include SharePoint and access-controlled file servers managed by Re: Sources IT. b. Use authorized secure sharing solutions if there is a business need to share information that is not allowed on DOJO Atlassian Tools with external parties. Examples of such services include LionBox, Vault, etc. c. Always ensure that the use of such DOJO Atlassian alternative tools in providing our services to our clients does not violate any contractual agreements with them.	

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Responsibilities

Stakeholders	Responsibilities
Global Security Office (GSO)	a. Develop, monitor, review and update these guidelines annually, or earlier as determined by business needs. b. Improve awareness and understanding of these guidelines within the Groupe via education and awareness programs. c. May ask Re:Sources IT to suspend without any prior notice any People's use of DOJO Atlassian Tools and/or remove or disable any content which is in violation of these guidelines or of the Groupe's policies, or applicable laws. d. Review the document classification level annually, or earlier as determined by business needs. e. Maintain the master copy of this document at the GSO portal. f. Publish or distribute the full or redacted version of this document to the intended recipients.
People	a. Read, understand and strictly adhere to these guidelines. b. Develop procedures as necessary to meet the requirements of these guidelines c. Agree that they are responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, written or audible communications of any nature stored and shared by People through DOJO Atlassian Tools. d. Do not share any password with any other person or authorize any other person to log onto their account. e. Inform the Global Security Office immediately of any unauthorized use of any account or content uploaded on DOJO Atlassian Tools that violates these guidelines and that comes to People's attention. f. Develop procedures as necessary to meet the requirements of these guidelines. g. Send an email to SecurityPolicies@publicisgroupe.com to submit any feedback for improvement or to ask any question related to these guidelines.
Groupe	a. Appoint a Champion within its organization to ensure that these guidelines are properly implemented to the brands or business units' staff. b. Champion is accountable to ensure that any requirements from Clients prohibiting the use of cloud-solutions for their engagement shall be notified and reported to the Global Security Office.

DOJO ATLASSIAN TOOLS ACCEPTABLE USE GUIDELINES

Revision History

Revision Date	Version	Summary of Changes	Approved by
August 9, 2016	1	Initial version.	Chief Information Security Officer, Publicis Groupe
February 27, 2017	1	Periodic Review.	Chief Information Security Officer, Publicis Groupe
January 4, 2018	1	Annual review, no changes needed.	Chief Information Security Officer, Publicis Groupe
January 04, 2019	1	Annual review, no changes needed.	Deputy Chief Information Security Officer, Publicis Groupe
January 02, 2020	1	Annual review, no changes needed.	Deputy Chief Information Security Officer, Publicis Groupe
January 02, 2021	1	Annual review, no changes needed.	Chief IT Security Officer, Publicis Groupe