TELEHOUSE

PO2 Information Security Management Policy

Document Control

Reference Number:	PO2
Document Title:	PO2 Information Security Management Policy
Version Number:	3.0
Date of Publication:	January 2016
Author:	J Slater
Filename:	PO2 Information Security Management Policy.doc
Number of Pages:	3 Including preliminaries

Document Version Control

Version / Status	Release Description	Date of Issue
0.1 Draft	Initial Draft	
1.0	Approval	28/01/2016
2.0	Review	25/01/2017
3.0	Change of MD	16/05/2017

TELEHOUSE

Telehouse Information Security Policy

KDDI European Bloc is committed to fully complying with the relevant laws and regulations in relation to Information Security ("Relevant Laws"), Protection of Personal Information and protecting the information assets from a wide range of infringement incidents and ensuring the confidentiality, integrity and availability of information assets of the Company.

The Bloc pursues a policy of continuous improvement, seeking every opportunity to identify risks, evaluate them and take action in line with ongoing efforts to grow our business.

For the aforementioned purpose, the Company will:

1) Establish a working structure in the Bloc to deal with Information Security.
2) Develop necessary internal rules to enforce this policy ("Enforcement Rules").
3) Check all the information assets and business processes, classify them and manage them properly.
4) Analyze threats to the information assets and business processes, their estimated probability, possible adverse impact on the Company's business and thus identify and assess the risks associated with them.
5) Develop the measures to manage and control the identified risks ("Control Measures") based on the aforementioned analysis and the assessment and put them into force.
6) Conduct a periodical and extraordinary internal audit on the Enforcement Rules and the Control Measures, etc. in terms of their effectiveness and enforceability, and based on the results of the audit, review, and, if it is deemed appropriate, amend this policy, the Enforcement Rules and/or the Control Measures or take any other step to ensure Information Security.
7) Take appropriate actions to enforce this policy as well as to apply Enforcement Rules to those who are not a Company's staff, but have an access to the information assets of the Company.
8) All Bloc staff shall have an adequate knowledge about the significance of Information Security and faithfully abide by all the provisions of the Enforcement Rules. Any actual or threatened infringement of the Relevant Laws or Enforcement Rules shall be reported to the management without delay.
9) Any noncompliance with the Relevant Laws or Enforcement Rules will be considered to be an offence, to which the Company's Disciplinary Procedures will apply.

Objectives

The corporate objectives in relation to Information Security are;

- To maintain the ISO27001 certification to add business value to Telehouse and the Bloc sales activities and support growth of the business
- Provide assurance for stakeholders and the Bloc companies as to how the information security is managed throughout the business.
- Prevent information leakage in Bloc business operations.

Signed 

Ken Sakai
Managing Director
Telehouse Europe

May 2017