NEBULA CONTROL CENTER GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is an agreement between Zyxel Communications Corp. ("Zyxel", "we", "us", or "our") and you or the entity you represent ("Customer", "you" or "your"). This DPA supplements the Terms of Use (the "Agreement") available at https://bulletin.nebula.zyxel.com/data-policies/NCC_TermsOfUse_20180731.en-us.html, as updated from time to time between Customer and Zyxel, or other agreement between Customer and Zyxel governing Customer's use of the service offerings when the GDPR applies to your use of the Nebula Control Center to process Personal Data. Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 16 of this DPA.

How to Execute this DPA:

This DPA has been pre-signed on behalf of Zyxel. To execute this DPA, please do as follow:

a) Please download this DPA, complete the form fields and sign on page 7.
b) Use Customer's email account to email the signed DPA to nebula-privacy@zyxel.com.tw.

Customer acknowledges and agrees that a completed and signed copy of this Agreement must be emailed, as indicated above, in order to become effective.

Once electronically executed by both the Customer and Zyxel, this DPA will be effective and your signatory will receive a confirmation email.

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Personal Data is processed by Zyxel. In this context, Zyxel will act as "processor" to Customer who may act either as "controller" or "processor" with respect to Personal Data (as each term is defined in the GDPR).

1.2 **Customer Controls.** The Nebula Control Center provides Customer with a number of controls including security features and functionalities that Customer may use to ensure the protection of Personal Data, deliver the corresponding statement of consent and regulate the scope of data processed (refer to Section 1.3.5). Without prejudice to Section 5, Customer may use these controls as technical and organisational measures to assist it in connection with its obligations under the GDPR.

1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Personal Data.

1.3.2 **Duration.** As between Zyxel and Customer, the duration of the data processing under this DPA is determined by Customer use of the Nebula Control Center.

1.3.3 **Purpose.** The principal purpose of the data processing under this DPA is the provision of the Nebula Control Center initiated by the Customer when logging into the Nebula Control Center portal. The Personal Data may be subject to the following basic processing activities: (a) customer service activities, such as processing orders, providing technical support and improving products, (b) delivery of the Nebula Control Center monitoring capabilities and services through which Customer manages and configures the Zyxel networking hardware devices.

1.3.4 **Nature of the processing:** All the Zyxel networking hardware devices that

are manageable through the Nebula Control Center are built with the capability to collect Personal Data from the network, sending it to the Nebula Control Center system for computing, formatting and storage. The data processing will be initiated by the Customer through deployment of the Zyxel networking hardware devices and integrating them to the Nebula Control Center.

1.3.5 **Type of Personal Data:** The Nebula Control Center collects the personal data on behalf of Customer, which may include the following categories and can be modified through Customer Controls:

- Email of the Customer and other personnel managing the Nebula Control Center portal; used for authentication, maintenance notifications and marketing bulletins about the Nebula Control Center (always).
- The IP Addresses of Data Subjects, in order to provide monitoring and network statistics to the Data Controller (always).
- Client hostname of Data Subjects, for the ease of network monitoring to Customer (always, but can be manually edited).
- Account information of Data Subjects using Nebula Control Center cloud hosted authentication server; for network authentication, monitoring and control (based on Customer Controls).
- Sign–on authentication username and/or email address of Data Subjects when using certain user authentication methods, including: active directory and radius servers; for network authentication, monitoring and control (based on Customer Controls).
- Data Subject's email, age, gender, locale when Facebook social login authentication is configured (based on Customer Controls). Please refer to Section 1.3.5.1 for details.
- Access destination and URL from a Data Subject's IP address by hitting firewall rules; for a network access control (based on Customer Controls).

1.3.5.1 Social Login: By default, The Nebula Control Center uses a Facebook App ID that is owned by Zyxel to facilitate the implementation of the Facebook social login authentication. Nebula Control Center's default Facebook App ID will only allow Data Subjects of 16 years old or older. As part of the Customer Controls provided by Nebula Control Center, Customer can also specify a self-created Facebook App ID, which could include a different age restriction.

1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools and APIs made available by Zyxel for the Services) constitute Customer's documented instructions regarding Zyxel's processing of Personal Data ("**Documented Instructions**"). Zyxel will process Personal Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Zyxel and Customer, including agreement on any additional fees payable by

Customer to Zyxel for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Zyxel declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.`

3. **Confidentiality of Personal Data.** Zyxel will not access or use, or disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Zyxel a demand for Personal Data, Zyxel will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Zyxel may provide Customer's basic contact information to the government body. If compelled to disclose Personal Data to a government body, then Zyxel will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Zyxel is legally prohibited from doing so.

4. **Confidentiality Obligations of Zyxel Personnel.** Zyxel restricts its personnel from processing Personal Data without authorisation by Zyxel as described in the Zyxel Security Standards. Zyxel imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. **Security of Data Processing.** Zyxel has implemented and will maintain the technical and organisational measures for the Nebula Control Center as described in the Zyxel Security Standards and this Section. In particular, Zyxel has implemented and will maintain the following technical and organisational measures:

   (a) security of the Nebula Control Center as set out in Section 1.1 of the Zyxel Security Standards;

   (b) measures to control access rights for Zyxel employees and contractors in relation to the Nebula Control Center as set out in Section 1.1 of the Zyxel Security Standards; and

   (c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by Zyxel as described in Section 2 of the Zyxel Security Standards.

6. **Sub-processing.**

   6.1 **Infrastructure Subprocessors – Service Data Storage.** Zyxel uses the following organisations to store/host/collect Personal Data, or provide other infrastructure that helps with delivery of the Nebula Control Center Service. These are secure environments that are controlled by the Zyxel team and are protected by Data Processing Agreements:

Entity Name	Purpose	Entity Country
Amazon Web Services, Inc.	Cloud Service Provider	Ireland

   6.2 **Authorised Sub-processors.** Customer agrees that Zyxel may use sub-processors to fulfil its contractual obligations under this DPA or to provide certain services on

its behalf. Customer consents to Zyxel's use of sub-processors as described in previous Section and agrees that Zyxel may engage any other third parties from time to time, with due notification, to process Personal Data in connection with making the Products available to Customer. If Customer objects to Zyxel's use of a new Sub-processor, Customer may terminate any Hosted Software Licenses in respect of only those Products that cannot be provided by Zyxel without the use of the objected-to new Sub-processor (the "New Sub-processor"), by providing written notice to Zyxel within a reasonable period of time following the notification, such period not to exceed thirty (30) days (the "Notice Period"); provided, that Zyxel will not be prohibited from engaging the New Sub-processor during or after the Notice Period

Except as set forth in this Section, or as Customer may otherwise authorise, Zyxel will not permit any sub-processor to carry out other processing activities on Personal Data on behalf of Customer.

6.3 **Sub-processor Obligations.** Where Zyxel authorises any sub-processor as described in Section 6.1:

(i) Zyxel will restrict the sub-processor's access to Personal Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the documentation and Zyxel will prohibit the sub-processor from accessing Personal Data for any other purpose;

(ii) Zyxel will enter into a written agreement with the sub-processor and, to the extent that the sub-processor is performing the same data processing services that are being provided by Zyxel under this DPA, Zyxel will impose on the sub- processor the same contractual obligations that Zyxel has under this DPA; and

(iii) Zyxel will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause Zyxel to breach any of Zyxel's obligations under this DPA.

7. Data Subject Rights. Zyxel will, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, restriction, portability, or deletion of such Data Subject's Personal Data. Except as required by law, Zyxel will not respond to any such Data Subject request without Customer's prior written consent. Taking into consideration the nature of the Processing, Zyxel will assist Customer through reasonable and appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request to the extent Zyxel is legally permitted to do so and the response to such Data Subject request is legally required. To the extent legally permitted and outside the ordinary course and cost of business, Customer is responsible for the costs associated with any such assistance provided by Zyxel.

Customer may reach us to evacuate any concern at privacy@zyxel.com.tw.

8. Security Breach Notification.

8.1 **Security Incident.** Zyxel will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

8.2 **Zyxel Assistance.** To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, Zyxel will include in the notification under Section 8.1(a) such information about the Security Incident as Zyxel is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Zyxel, and any restrictions on disclosing the information, such as confidentiality.

8.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 8. An unsuccessful Security Incident is one that results in no unauthorised access to Personal Data or to any of Zyxel's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) Zyxel's obligation to report or respond to a Security Incident under this Section 8 is not and will not be construed as an acknowledgement by Zyxel of any fault or liability of Zyxel with respect to the Security Incident.

8.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Zyxel selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information and secure transmission at all times.

9. Zyxel Certifications and Audits.

9.1 **Zyxel ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, Zyxel will make available the following documents and information:

(i) the certificates issued in relation to the ISO 27001 certification, the ISO 27017 certification and the ISO 27018 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017 and ISO 27018); and

(ii) the System and Organisation Controls (SOC) 1 Report, the System and Organisation Controls (SOC) 2 Report and the System and Organisation Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by Zyxel that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

9.2 **Zyxel Audits.** Zyxel uses external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at Zyxel's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be Zyxel's Confidential Information.

9.3 **Audit Reports.** At Customer's written request, and provided that the parties have

an applicable NDA in place, Zyxel will provide Customer with a copy of the Report so that Customer can reasonably verify Zyxel's compliance with its obligations under this DPA.

9.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the Services and the information available to Zyxel, Zyxel will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, by providing the information Zyxel makes available under this Section 9.

10. Customer Audits. Customer agrees to exercise any right it may have to conduct an audit or inspection, by instructing Zyxel to carry out the audit described in Section 9. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Zyxel written notice. If Zyxel declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement.

11. Transfers of Personal Data.

11.1 **Location.** The datacentre that holds Personal Data processed by Nebula Control Center is located in Dublin, Ireland, EEA.

11.2 **Transfer out of the EU.** Zyxel does not and will not transfer nor copy Personal Data outside of the EEA, except as necessary to comply with the law or binding order of a governmental body.

12. Termination of the DPA. This DPA shall continue in force until the termination of the Agreement (the "**Termination of Usership**"). For avoidance of doubt, this DPA shall only become legally binding between Customer and Zyxel when the steps set out in the Section "How to Execute this DPA" above have been fully completed.

13. Return or Deletion of Personal Data. At the termination of the Agreement, upon Customer's written request and within a reasonable period, Zyxel will: (i) make available to Customer all Personal Data, or (ii) delete, restrict processing, and/or de-identify Personal Data, including Personal Data, in such a way as to render such data inaccessible and unidentifiable to Customer or any third party. Unless such return, deletion, restriction of processing, or de-identification is not feasible or continued retention and processing is required or permitted by applicable law, Zyxel will respond to such request as soon as reasonably practicable.

14. Duties to Inform. Where Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Zyxel, Zyxel will inform Customer without undue delay. Zyxel will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Personal Data subjected to those proceedings is Customer's property and area of responsibility and that Personal Data is at Customer's sole disposition.

15. Entire Agreement; Conflict. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control.

16. Definitions. Unless otherwise defined in the Agreement, all capitalised terms used in this DPA will have the meanings given to them below:

"Nebula Control Center" means the Nebula SaaS including networking devices and cloud system provided by Zyxel, covered in this DPA and to which the Customer is accessing.

"Zyxel Security Standards" means the security standards attached to this DPA as Annex 1.

"GDPR" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"EEA" means the European Economic Area.

"Customer" means you or the entity you represent.

"Personal Data" has the meaning given to it in the GDPR.

"Data Subject" means the individual to whom Personal Data relates.

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"Security Incident" means a breach of Zyxel's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

[Zyxel]

Signature 

Name Crowley Wu

Title Senior AVP, NSBU

Date Signed 2018/5/25

[Customer]

Signature _____

Name _____

Title _____

Date Signed _____

Annex 1

Zyxel Security Standards

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. **Information Security Program.** Zyxel will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Nebula Control Center, and (c) minimise security risks, including through risk assessment and regular testing. Zyxel will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The Nebula Control Center will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Zyxel will maintain access controls and policies to manage what access is allowed to the Nebula Control Center from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Zyxel will maintain corrective action and incident response plans to respond to potential security threats.

2. **Continued Evaluation**. Zyxel will conduct periodic reviews of the security of its Nebula Control Center and adequacy of its information security program as measured against industry security standards and its policies and procedures. Zyxel will continually evaluate the security of its Nebula Control Center and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.