# *Child Online Safeguarding*

***POLICY***

# Child Online Safeguarding Policy

*Document No.:* POL---  *Version. No. 1*

| | |
|---|---|
| *Governing policy:* | ***N/A*** |
| *Policy applies to:* | ☒ ***Company-wide*** ☐ ***Specific group or employees only*** |
| *Documented type:* | ☒ ***New*** ☐ ***Revision of existing documented information*** |
| *Policy document status:* | ☐ ***INITIAL DRAFT*** ☐ ***INITIAL REVIEW*** ☐ ***FINAL REVIEW*** ☒ ***APPROVED*** |

| | |
|---|---|
| *Policy / Process Control Review Authority:* | ***Corporate Governance and Data Privacy Group*** |
| *Compliance governance review owner:* | ***ORIGINAL SIGNED***<br>***John Michael C. Avila***<br>*Regulatory, Ethics, and Governance Lead* *Date:*_____ |
| *Data Privacy review owner:* | ***ORIGINAL SIGNED***<br>***Eumir Paolo C. Espiritu***<br>*Data Privacy Head* *Date:*_____ |
| *Compliance governance and Data Privacy review officer:* | ***ORIGINAL SIGNED***<br>***Atty. Laurice Esteban -Tuason***<br>*Sr. VP & Corporate Compliance/ Data Protection Officer* *Date:*_____ |
| *Network Operations review officer:* | ***ORIGINAL SIGNED***<br>***Paulo Martin G. Santos***<br>*EVP and Chief Network Transformation Officer* *Date:*_____ |
| *IT review officer* | ***ORIGINAL SIGNED***<br>***Ulysses C. Naguit***<br>*EVP and Chief Information Officer* *Date:*_____ |
| *Human Resources review officer* | ***ORIGINAL SIGNED***<br>***Albert Benjamin R. Custodio***<br>*Sr. VP & Head of Human Resources* *Date:*_____ |
| *Corporate Communications review officer:* | ***ORIGINAL SIGNED***<br>***Jay-Anne R. Encarnado***<br>*VP and Head of Corp. Communications and PR* *Date:*_____ |
| *Enterprise Risk Management review officer:* | ***ORIGINAL SIGNED***<br>***Jerome Mario T. Orfano***<br>*VP and Head of Enterprise Risk Management* *Date:*_____ |

# Child Online Safeguarding Policy

*Document No.:* POL--- *Version. No. 1*

| | |
|---|---|
| *Strategy Management and Transformation review officer:* | ***ORIGINAL SIGNED***<br>***Benjamin Rex Emilio B. Azada***<br>*EVP and Chief Strategy Officer* *Date:*_____ |
| *Executive approval authority:* | ***ORIGINAL SIGNED***<br>***Grace Y. Uy*** *Date:*_____<br>*President and Chief Risk Officer*<br>***ORIGINAL SIGNED***<br>***Amando M. Tetangco, Jr.***<br>*Chairman of the Board Risk Oversight Committee* *Date:*_____ |

| | |
|---|---|
| *Implementation effectivity date:* | ***November 2022*** |
| *Approval Date of last revision* | ***N/A*** |
| *Effectivity Date of last revision* | ***N/A*** |
| *Date of governing policy review** | ***November 2022*** |

***Unless otherwise indicated, this policy shall apply beyond the review date***

| | |
|---|---|
| *Related legislation, standards, policies, procedures, guidelines, and local protocols* | **External References:**<br><br>Republic Act (R.A.). 11930 – Anti Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act<br>R.A. 10175 – Cybercrime Prevention Act of 2012<br>R.A. 9775 - Anti-Child Pornography Act of 2009 (as repealed by R.A. 11930)<br>National Cybersecurity Plan of 2022<br>National Study on Online Sexual Abuse or Exploitation of Children in the Philippines<br>National Institute of Standards and Technology Cybersecurity Framework (NIST) as adopted by the Department of Information and Communications Technology in its National Cybersecurity Plan<br>Computer Energy Response Team (CERT) -PH Incident Reporting and Technical Assistance Request Guidelines<br>Anti-Money Laundering Council Study - Online Sexual Exploitation of Children: A Crime with a Global Impact and an Evolving Transnational Threat<br>UN Convention on the Rights of the Child<br><br>**Internal References:**<br><br>Code of Business Ethics - POL-SARC-QRMS-1007<br>Employee Discipline Policy - CICT-HR POLICY-001<br>Personal Data Protection Policy - POL-IT-DP-001<br>Information Security Policy - POL-PQM-ISM-005<br>Whistleblowing Policy - POL-SARC-QRMS-1011<br>Whistleblowing Procedure - PRO-CGDP-BCM-0002<br>Enterprise Risk Management Policy - POL-ERMG-ERM-0001 ERM-0001<br>Human Rights Policy – POL – CGDP – REG – 0001 |

# Child Online Safeguarding Policy

*Document No.:* POL---  *Version. No. 1*

## Table of Contents

# 1. Introduction

In the advent of digitalization, the online space has been a platform for a bustling economy; opening a gateway for the advancement and expansion of businesses, enterprises, and individual endeavors. Rapid digital transformation has changed the way the internet is being used and consumed. With this rapid growth, there's bound to be those who will use any means to exploit and manipulate new technology to serve their selfish and nefarious purposes, be they individuals or more organized entities. Unknowing users, especially children, are left vulnerable to threats, attacks, and exploitative intentions.

# 2. Purpose

As the leading fiber powered Internet Service Provider (ISP) in the Philippines, Converge Information and Communications Technology Solutions, Inc. ("Converge") mandates itself to promote and foster a safer internet experience for its customers and end-users, particularly children who are vulnerable to malicious content, cyber-attacks, and online exploitation. Converge has established this policy to combat threats targeting children and build effective prevention and control measures within Converge's network. Through the implementation of this policy, we aim to uphold the rights of children and protect them against OSAEC/CSAEM, cyberattacks (including financial fraud) or online schemes targeting children. This policy signifies our commitment to act on negative impacts brought about by the misuse and abuse of digital space, as specifically targeting children.

# 3. Scope

The Child Online Safeguarding Policy shall apply to all employees of Converge, as well as its subsidiaries, Metroworks ICT Construction Inc. and Pentagon Holding Co. Inc., and its affiliates, (collectively referred to herein as "Company"), who are enjoined to adhere to the policy statements in this document.

In addition, relevant stakeholders such as but not limited to customers, investors, suppliers, vendors, business partners, third-party intermediaries, and communities are expected to embody the same principles enshrined in our policy statements.

# 4. Definitions

Please refer to **Annex A** for the glossary of terms used in this policy.

# 5. Policy Statements

## 5.1 Our Commitments

### 5.1.1 As an organization and ISP

The Company commits to respect the rights of our stakeholders, particularly children, who are highly vulnerable to digital threats. We shall adhere to all applicable child protection laws and utilize our resources in the implementation of internal controls to address negative impacts and identified threats.

#### 5.1.2 To our stakeholders and the community

We commit ourselves to ensure that our stakeholders, especially children are afforded proper digital safety and security in their use of our products and services. We commit to actively engage with our stakeholders and involve them in our anti-OSAEC/CSAEM and cybersecurity awareness initiatives. We also commit to work with relevant law enforcement agencies and government bodies to provide them with necessary support and information, as may be mandated for by law.

#### 5.1.3 To children victims

We shall continue implementing all necessary controls and safeguards to prevent any child from being victimized. We shall help promote digital literacy and awareness on anti-OSAEC/CSAEM and cyber fraud. We commit that our network shall not be misused and abused, nor will it be a medium for the proliferation of any malicious, demeaning, exploitative, fraudulent, or unethical activity.

### 5.2 Policy Framework

The Company is certified under and compliant with the requirements of ISO: 27001:2013 or the International Standard for Information Security Management Systems. We also adopt a combined framework recommended by the National Study on Online Sexual Abuse and Exploitation of Children in the Philippines (NS-OSAEC)[1], and the Cybersecurity Framework of the National Institute of Standards and Technology (NIST)[2]. We likewise adhere to the principles of Confidentiality, Integrity, and Availability (CIA) to manage risks and threats related to cybercrimes affecting children. Below summarizes the principles of our framework:

- **Identification:** Involves a key understanding of the business, its resources, functions, and risks related to cybersecurity affecting children and OSAEC/CSAEM. The Company shall implement its risk

[1] National Study on the Online Sexual Abuse and Exploitation of Children - https://www.unicef.org/philippines/media/2711/file/UNIPH-2021-NationalStudyOSAEC-FullReport.pdf

[2] National Institute of Standards and Technology - Cybersecurity Framework - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

management and governance strategies to identify appropriate controls and risk treatment plans to address these risks.

- **Protection:** Entails the development of safeguards, and coordination with communities and government entities to ensure continuity of operations in addressing cybersecurity, OSAEC-CSAEM, and related risks affecting online safety of children. The Company shall ensure internal controls are executed and shall maintain an open line of communication with communities, law enforcement, like-minded private institutions, and other similarly functioning entities in order to protect children.

- **Detection:** Mandates the installation of available technology, program, or software[3], complemented by the utilization of external sources or open-sourced data from law enforcement to detect or intercept online threats affecting children, including but not limited to OSAEC-CSAEM, malicious activities, phishing, social engineering, other fraud, or cybercrimes, that intend to undermine our network's safety and security. The Company shall allocate resources to procure and implement detection technologies and explore partnerships with various institutions to further strengthen our network's capacity to detect and combat these online threats (i.e. OSAEC/CSAEM and phishing, malicious activities, social engineering and the like).

- **Response:** Requires the execution of controls and safeguards regarding online threats affecting children, including but not limited to OSAEC-CSAEM, malicious activities, phishing, social engineering, other fraud, or cybercrimes, that intend to undermine our network's safety and security. Our Company shall aid in providing reports to the authorities, provide technical assistance, and promote digital awareness.

- **Recovery:** Provides for the implementation of restitutive safeguards brought by the impact of online threats affecting children (including but not limited to OSAEC-CSAEM, malicious activities, phishing, social engineering, other fraud, or cybercrimes) to our conduct of business. The Company shall ensure that our services remain unaffected and that any impact thereto, be resolved immediately with little to no interruption of service.

In view of the foregoing, the Company will adopt progressive recommendatory frameworks, such as DICT's National Cybersecurity Plan, and related ISO/IEC 27001:2013, ISO/IEC 27032:2012 standards. We shall move dynamically to be at the forefront of evolving digital and cybersecurity landscapes.

[3] Republic Act 11930 - Anti-OSAEC/CSAEM Act, Sec. 9 (6)

## 6. Key Focus Areas

As we stand firmly against any form of abuse to children, we give paramount importance to the following key areas that reflect how we do business.

### 6.1 Rights of Children

The Company shall uphold, respect, and protect the rights of children. We deem that it is our responsibility to foster and establish a safer internet experience for our users, especially children. We do this by raising awareness, monitoring, and filtering content, following legislation, coordinating with government bodies, and collaborating with like-minded organizations.

### 6.2 Legal and Governmental

The Company adheres to the provisions of the Cybercrime Prevention Act of 2012 and Anti-OSAEC/CSAEM Act, and other related legislation that provides for our responsibilities as an ISP in curbing, mitigating, and preventing any form of cyber abuse and exploitation of children. In compliance with regulations, Converge shall, among others[4]:

- Block access or filter websites and contents that contain or relate to any form of OSAEC/CSAEM, and child-pornography, pursuant to lawful orders or government requests, guided by our internal policies on content/site blocking.
- Provide reports, responses, information, and notifications to competent authorities which contain the actions we have taken to block, filter, and address OSAEC/CSAEM. Our reports shall also include the list of contents or websites blocked by our network. We shall likewise report any identifiable OSAEC/CSAEM related financial transactions or activities done through our network, as the case may be[5].
- Preserve traffic, content, and computer data, including logs that relate to any potential or actual OSAEC/CSAEM offense, pursuant to a lawful order. Our data collection and preservation shall be guided by existing laws and the Data Privacy Act of 2012.
- Leverage governance controls and communication channels which includes creation of additional policies and our coordination with government bodies to combat OSAEC/CSAEM.

[4] Republic Act 11930 - Anti-OSAEC/CSAEM Act, Sec. 9

[5] Anti-Money Laundering Council Study - Online Sexual Exploitation of Children: A Crime with a Global Impact and an Evolving Transnational Threat - http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf

- Provide explicit provisions in our service agreements, terms of service, and any other related document, that the Company prohibits any form or conduct of OSAEC/CSAEM in the use of our services.
- Institute, install, and implement programs, software, and solutions, in accordance with the provisions of the above laws.
- Comply with international treaties concerning the rights of children to which the Philippines is a signatory.
- Address financial fraud through proper information sharing with financial institutions or government bodies that combat any form of financial fraud designed to target children, which aims to exploit and extort them for undue financial benefit. This includes complying with any existing regulatory and legislative mandates to takedown, block, and report any malicious, fraudulent, phishing, and financially exploitative sites or platforms that use children as means to proliferate or fund activities relating to financial fraud. With this, we shall equip our network with detective and preventive cybersecurity measures that will aid financial institutions and government bodies in their fraud investigations and fraud prevention initiatives.

### 6.3 Data Privacy and Protection

The Company is a Personal Information Controller (PIC) that follows the general data privacy principles of transparency, proportionality, and legitimate purpose. It is our responsibility to manage information sharing and ascertain its legitimacy. In aiding organizations, law enforcement, and government agencies, we shall consider provisions on data and information sharing, as may be provided by the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

Specifically, in processing or reporting OSAEC/CSAEM related activities, we shall be transparent, yet prudent in disclosing personal information. We recognize the importance of privacy in order to avoid any reprisals or ostracizing behavior towards any person. Our privacy controls, being based on the issuances of the National Privacy Commission (NPC), shall balance the required disclosures with the basic right of a person to privacy.

We conduct all necessary privacy awareness training to our stakeholders, and we implement controls that safeguards a person's privacy.

### 6.4 Information Security

The Company shall maintain the confidentiality, integrity and availability of its information and assets in compliance with the Information Security Policy and the ISO/IEC 27001:2013 or Information Security Management System standards.

We have instituted policies and controls which are aligned with our internal network policies to combat OSAEC/CSAEM activities and cyber fraud attacking children. To this effect, we shall continue to filter or block any malicious content (i.e. CSAEM), phishing sites, provide awareness initiatives to our employees and stakeholders, and promote digital literacy.

We ensure our stakeholders that our network and information security controls will enable users, specifically children, to have a safe digital experience. We also commit to strengthen our cybersecurity resources and implement dynamic measures that will progressively keep us abreast with the evolving digital space.

### 6.5 Community and stakeholder relations

We recognize our responsibilities as an ISP in the communities where we operate. We commit to utilize our technology to address online threats affecting children, including but not limited to OSAEC-CSAEM, malicious activities, phishing, social engineering, other fraud, or cybercrimes. We shall ensure continuous collaboration with the government, NGOs, private institutions, financial institutions, non-profit organizations, and government bodies to implement the provisions of the relevant laws that relate to the protection of children against cyber-abuse and exploitation.

To this effect, we shall conduct relevant training and awareness programs and direct a portion of our Corporate Social Responsibility (CSR) initiatives to focus on Anti-OSAEC/CSAEM and Fraud Prevention partnerships. The Company holds a commitment to only engage with ethical and likeminded entities.

We implore our stakeholders to be vigilant and responsible. We urge them to aid us to stop the proliferation and cultivation of any offenses targeting children.

### 6.6 Financial Protection and Digital Literacy

The Company considers financial protection and digital literacy as key factors in mitigating and eliminating financial fraud targeting the vulnerability of children. We recognize that children, having digital access at such a young age, are susceptible to potentially harmful digital content, including financial fraud, with little to no restriction or awareness, especially if left unsupervised. Relatedly, exploitative intents are now being channeled through social media, online games and portals, chatroom platforms, among others, followed by

attempts of phishing and other similar social engineering methods. These methods and platforms serve to be triggers in the exploitation of children in the commercial and financial purview as children are being coerced, blackmailed, brainwashed, or threatened to provide undue financial benefit to individuals or criminal organizations/syndicates, which these wrongdoers then use to facilitate business transactions where children are considered capital and source of financing.

To this effect, the Company commits to promote, raise awareness, and aid in activities related to the financial protection and digital literacy of children and their families so that they are afforded proper knowledge on how to detect, recognize, and act on these financial fraud threats. We shall also consider collaborating with online platforms and financial institutions in establishing safeguards and blocking phishing and social engineering sites, particularly when such platforms are being accessed through our network. We commit to aid government authorities in addressing commercial and financial activities used to exploit children.

### 6.7 Employee involvement

Pursuant to the provisions of our Code of Business Ethics (CoBE) policy, we mandate our employees to uphold the provisions of this policy. Our employees are expected to be our stewards in ensuring that OSAEC/CSAEM and cybercrime in general, will not proliferate both in the workplace and in their personal capacities. We enjoin our personnel to participate in awareness campaigns and outreach programs designed to promote the safety and security of our network. We expect our employees to be vigilant and report any identified infractions or offenses. We urge our employees to reach out to law enforcement should they be aware of any such situation.

### 6.8 Governance

The Company shall uphold its responsibilities as an ISP. We shall promote, implement, and supplement all applicable mandates under the Cybercrime Prevention Act, Anti-OSAEC/CSAEM Act, regulations relating to financial fraud, and any other legislation related thereto. We ensure that our products and services, particularly our network, are well equipped with protective safeguards that will identify, prevent, and resolve any related threats or attacks targeting children and that intend to undermine our network's safety and security.

In addressing such threats or attacks, we shall coordinate with government agencies and regulatory bodies to ensure that children and our stakeholders are well protected and that their rights are upheld. Correspondingly, we shall not tolerate any form of cyber abuse targeting children from any of our

stakeholders. Should there be reports relating to such cyber abuse, the Company shall provide reporting channels to address such infractions. Specifically, on OSAEC-CSAEM, we guide our stakeholders to submit any concern or infraction to the National Coordination Center against OSAEC and CSAEM (NCC-OSAEC-CSAEM)[6], the Inter-Agency Council Against Trafficking (IACAT), Philippine National Police (PNP), National Bureau of Investigation (NBI), the Department of Justice (DOJ), Computer Energy Response Team (CERT) -PH and/or all other similarly functioning government entities and reporting channels.

We shall not hesitate to coordinate with proper authorities and provide them with necessary reports and information, in accordance with law. We assure our stakeholders that our Network Operations (NetOps) Group, together with our Information Security Team, shall be at the forefront of executing internal controls to ensure that our services will not be used to proliferate cyber abuse targeting children.

## 7. Implementation and Monitoring

Our NetOps Group shall act as the primary oversight in ensuring that the provisions of this policy be implemented and monitored across the organization. Business units tagged by the NetOps Group as support drivers, are enjoined to ensure that all activities and responsibilities mentioned herein are well communicated and executed.

The Corporate Governance and Data Privacy (CGDP) Group of the Company shall be responsible for mapping out our compliance responsibilities as an ISP. These responsibilities shall include tasks and mandates from all applicable laws and regulations.

The Company's Sustainability Council, along with its Business Unit Partners shall support both the NetOps Group and CGDP group in the implementation and monitoring of this policy.

## 8. Communication

The Company is committed to communicate and implement this policy to both internal and external stakeholders. We shall integrate the NIST - NS OSAEC framework throughout our operations. In full transparency, we shall reflect how we uphold our commitments in our related company documents, reports, and publications.

Upon approval of the Child Online Safeguarding Policy, The Corporate Governance and Data Privacy Group, is tasked to immediately disseminate and enforce this policy, company-wide. It should be noted however that the

[6] Republic Act 11930 - Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

primary responsibility of ensuring that the provisions of this policy are operationalized rests with the NetOps Group and supporting business unit partners.

## 9. Non-Compliance and reporting process

We expect our personnel, third-party intermediaries, business partners, and other relevant stakeholders to aid us in preventing, identifying, and responding to any cybercrime affecting children or OSAEC/CSAEM related infractions. Anyone found to have violated this Child Online Safeguarding Policy, in relation to the course of our operations, products, and services shall be dealt with in accordance with local legislation, supported by our internal policies and procedures.

An employee found to have violated the provisions of this Child Online Safeguarding Policy shall be subjected to disciplinary action in accordance with the Company's Employee Discipline Policy.

Any person, with knowledge of, or has observed, any act which may be considered as an offense under the Cybercrime Prevention Act, Anti-OSAEC/CSAEM Act, and other related online crimes targeting children may choose to file a report to the proper authorities or through the whistleblowing reporting channels for immediate attention. Further details on how the Company handles reports can be found in its Whistleblowing Policy and Whistleblowing Procedure documents.

## 10. Related document references

Please see the cover page for the breakdown of reference documents.

## 11. Details of revision/s made to this policy

From time-to-time the Company may amend this Policy and set out relevant guidelines to continuously improve its suitability, adequacy, and effectiveness.

| Version No. | Date | Description of Change | Author | Approver |
|---|---|---|---|---|
| 1.0 | November 2022 | Initial policy draft | JM Avila | Please see cover sheet for the list of approvers |

## 12. Annex

Annex A - Glossary of terms used in this policy.

| Term | Definition |
|---|---|
| Child / Children | Is a person under the age of eighteen (18) years or those over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation or discrimination because of physical, mental, intellectual or sensory disability or condition.[7] |
| Child Sexual Abuse and Exploitation Materials (CSAEM) | Any representation, whether offline, or by, through, and with the use of information and communications technology, whether visual, video, audio, written, or any combination thereof, by electronic, mechanical, digital, optical, magnetic, or any other means, depicting acts of sexual abuse or exploitation.[8] |
| Competent authority | Refers to law enforcement authority, investigating authority, prosecutor, court, telecommunications/ICT regulator, or the National Coordination Center against OSAEC and CSAEM.[9] |
| Computer data | Any representation of facts, information, or concepts in a form suitable for processing in a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.[10] |
| Computer Energy Response Team (CERT) -PH | A group under the DICT that handles computer security incidents. CERT-PH is responsible for receiving, reviewing, and responding to computer security incident reports and activities.[11] |
| Content data | The content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data, or subscriber's information/registration information.[12] |
| Cyber | A computer or a computer network, the electronic medium in which online communication takes place[13] |

[7] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (a)

[8] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (c)

[9] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (e)

[10] R.A. 10175 - Cybercrime Prevention Act of 2012, Sec. 3 (e)- https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf

[11] CERT-PH profile - https://www.ncert.gov.ph/wp-content/uploads/2020/12/CERT-PH-RFC2350-Profile.docx.pdf

[12] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (h)

[13] R.A. 10175 - Cybercrime Prevention Act of 2012, Sec. 3 (i) - https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf

| Term | Definition |
|---|---|
| Cybercrime | Offenses against the confidentiality, integrity, and availability of computer data and systems[14] |
| Cybersecurity | The collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.[15] |
| Department of Information and Communications Technology (DICT) | The executive department of the Philippine government responsible for the planning, development and promotion of the country's information and communications technology agenda in support of national development. |
| DICT - Cybersecurity Plan | Strategies intended to shape the policy of the government on cybersecurity and the crafting of guidelines that will be adapted down to the smallest unit of the government. It also intends to provide a coherent set of implementation plans, programs, and activities to be shared to the public and private sector, the civil society, and the academe, including the private individuals. |
| Internet Intermediary | Persons or entities that provide infrastructure, platforms, access to, and host, transmit and index content, products and services originated by third parties on the internet.[16] |
| Internet Service Provider (ISP) / Service Provider | A public telecommunication entity (PTE) or value-added service (VAS) provider duly authorized by or registered with National Telecommunications Commission (NTC) that provides users or other entities with data connections allowing access to the internet through physical transport infrastructure, and such access is necessary for internet users to access content and services on the internet, and for content providers to publish or distribute materials online.[17] |

[14] R.A. 10175 - Cybercrime Prevention Act of 2012, Sec. 4 (a) - https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf

[15] R.A. 10175 - Cybercrime Prevention Act of 2012, Sec. 3 (k) - https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf

[16] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (p)

[17] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (q)

| Term | Definition |
|---|---|
| National Coordination Center against OSAEC and CSAEM (NCC-OSAEC-CSAEM) | A coordination center reporting under the Inter-Agency Council Against Trafficking (IACAT) that is tasked to develop and implement necessary programs that will prevent the commission of OSAEC and CSAEM, as well as protect, heal and reintegrate the child into the mainstream of society. |
| National Institute of Standards and Technology (NIST) Cybersecurity Framework | A voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The framework is also designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. |
| National Privacy Commission (NPC) | A government body mandated by the Data Privacy Act of 2012 to administer and implement provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection. |
| National Study on Online Sexual Abuse and Exploitation of Children in the Philippines (NS-OSAEC) | A data-driven guide for policy makers and various stakeholders who are invested in preventing and combating OSAEC.[18] |
| National Telecommunications Commission (NTC) | The attached agency of the DICT, responsible for the supervision, adjudication and control over all telecommunications services and television and radio networks throughout the Philippines. |
| Online Sexual Abuse and Exploitation of Children (OSAEC) | The use of ICT as a means to abuse and/or exploit children sexually, which includes cases in which offline child abuse and/or exploitation is combined with an online component.[19] |

[18] https://www.unicef.org/philippines/media/2711/file/UNIPH-2021-NationalStudyOSAEC-FullReport.pdf

[19] R.A. 11930 - Anti- Online Sexual Abuse or Exploitation of Children and Anti- Child Sexual Abuse or Exploitation Materials Act , Sec. 3 (t)

| Term | Definition |
|---|---|
| Phishing | A cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.<br><br>The information is then used to access important accounts and can result in identity theft and financial loss[20]. |
| Social Engineering | An attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.<br><br>Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data[21]. |
| Traffic data | Any computer data other than the content of communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[22] |

[20] https://www.phishing.org/what-is-phishing

[21] PNP – Anti-Cybercrime Group Security Bulletin NR 69 - https://pnpacg.ph/main/cyber-security-bulletin/150-acg-cyber-security-bulletin-nr-69-social-engineering-in-gaining-access-to-data.html

[22] R.A. 10175 - Cybercrime Prevention Act of 2012, Sec. 3 (e)- https://www.officialgazette.gov.ph/downloads/2012/09sep/20120912-RA-10175-BSA.pdf