मितिः २०७८/०५/०४ (20 August, 2021)

# साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

## कुकिज सुरक्षा (Cookies Security) संग सम्बन्धितः

### (१) कुकिज (Cookies) के हो?

कुनै Website Browse गर्दा उक्त Web Server ले प्रयोगकर्ताको Device वा Web Browser मा राख्ने सानो Text File/Data लाई Cookies (or, Internet Cookies) भनिन्छ। यो मुख्यत: Internet प्रयोगकर्ताको Username, ID, Email, Preference जस्ता विवरणहरु Save गरी राम्रो इन्टरनेट अनुभुतिको लागि प्रयोग गरिन्छ। यसलाई Session Management, Personalization र Tracking(User/Device) गर्ने प्रयोजनको लागि प्रयोग गरिन्छ। Cookies मुख्यतः निम्न प्रकारका हुन्छन् - Session Cookies, Persistent Cookies, Third-Party Cookies, Super Cookies, Zombie Cookies।

### (२) कुकिज (Cookies) ले कसरी काम गर्छ ?

कुनै वेबसाइट पहिलो पटक Browse/Visit गर्दा प्रयोगकर्ताको कम्प्युटरमा उक्त वेबसाइटबाट प्रयोगकर्ताको अनुमति लिई वा नलिई Cookies Download र Save भएर बस्छ। अर्को पटक उक्त वेबसाइट Browse/Visit गर्दा Save भएर बसेका Cookies (Unique ID) मार्फत प्रयोगकर्ताको विवरण Server ले सजिलै प्राप्त गरी इन्टरनेट प्रयोगानुभुति बढाउन मद्दत गर्छ। Cookies मार्फत प्रयोगकर्ताको Browsing Behavior लाई Track गरी प्रयोगकर्ता सुहाउँदो विज्ञापन पठाउने गर्दछ।

### (३) कुकिज (Cookies) बाट हुन सक्ने जोखिम के के हुन?

साधारणतया सबै वेबसाइटमा Browse/Visit गर्दाको बखत Accept Cookies भनी प्रयोगकर्ताको सहमति माग्ने गर्छन्। कुनै वेबसाइटमा Accept Cookies लाई "Yes" भनी सहमति दिंदा उक्त वेबसाइटसंग आबद्द रहेको Third Party ले समेत Save भएर रहेको विवरणमा पहुँच पाउँछ। यसरी कुकिजले Store गर्ने विवरण साधारणतयाः Plain Text मा हुने भएकोले एउटा वेबसाइटको लागि Save भएर रहेको संवेदनशील विवरणमा (User Credentials, Bank Details, Personal Information etc) अर्को वेबसाइटको कुकिज मार्फत साइबर अपराधीले सजिलै cross site scripting गरी विवरणहरु चोर्न सक्छन्। तसर्थ Cookies

बाट हाम्रो गोपनियता भंग हुने र Security Threat रहने जोखिम हुन्छ। साथै प्रयोगकर्ताको गतिविधि तथा आनीबानीलाई साइबर अपराधीले Cookies को डाटा मार्फत Track गर्न सक्छ।

## (४) कुकिज (Cookies) वाट हुन सक्ने साइबर हमलावाट कसरी बच्ने ?

Cookies बाट हुन सक्ने साइबर हमलावाट बच्न निम्न उपायहरु अपनाऔ :-

१. वेबसाइटहरु Browse/Visit गर्दा Cookies हरुलाई नपढी सहमति प्रदान नगरौं।

२. वेबसाइटले प्रदान गर्ने कुकिजलाई सर्वप्रथम राम्रोसंग पढेर Customize गरौं।

३. कुकिजको लागि सहमति नमाग्ने वेबसाइटहरु सुरक्षा खतरा भए / नभएको पहिचान गरी Browse/Visit गरौं।

४. Trusted Website तथा Https/Lock Sign भएको वेबसाइटको मात्र प्रयोग गरौं।

५. Browser मा उचित तरिकाले Cookies को Setting लाई Configure गरौं। आफुले प्रयोग गर्ने Browser को Privacy Settings मा रहेको "Do not Track" जस्ता Option को प्रयोग गरौं।

६. मोबाईलमा Third Party मार्फत सजिलै Track हुन सक्ने भएकोले सकेसम्म मोबाईलबाट हुने Web Browse लाई सिमीत गरौं।

७. सम्भव भएसम्म एउटै Browser को प्रयोग नगरौं। बैंकिङ्ग कारोबार लगायतको कार्य गर्दा सुरक्षित Browser (जस्तैः Mozilla Firefox)को प्रयोग गरौं।

८. Internet चलाउँदा Browser को Private Browsing Mode को प्रयोग गरौं।

९. समय समयमा आफ्नो Browser मा भएको Cookies तथा Site Data हरुलाई Clear गरौं।

१०. कुनै वेबसाइटमा Login गरेको भएमा काम सकिने बितिक्कै Log Out गर्ने गरौं।

११. Browser मा विश्वाशिलो Ad-Block गर्ने तथा Securely Browse गर्ने Plugin हरुको प्रयोग गरौं।

१२. आफ्नो कम्प्युटर, मोबाइल आदिमा Internet Security Software को प्रयोग गरौं।

**Nepal Telecommunications Authority (NTA)**
**Cyber Security Task Force (NTACERT)**
**Jamal, Kathmandu, Nepal**
**Email: cert@nta.gov.np, Website: www.nta.gov.np**