भारतीय बीमा नियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA

साइबर सुरक्षा घटना की सूचना देने का प्रोफार्मा
CYBER SECURITY INCIDENT REPORTING PROFORMA

साइबर सुरक्षा घटना की सूचना और रिपोर्टिंग प्रोफार्मा निम्नलिखित को भेजा जाएगा:
The intimation of Cyber Security incident and the reporting proforma shall be sent to:
infosec@irdai.gov.in

आधारभूत विवरण	
संस्था का नाम	
सूचना देनेवाले व्यक्ति का नाम	
पदनाम और विभाग	
कार्यालयीन ई-मेल आईडी	
टेलीफोन / मोबाइल संख्या	
घटना की सूचना निम्नलिखित को देने की तारीख और समय लिखें	आईआरडीएआईः
	सर्ट-इनः
	क्या घटना की सूचना सर्ट-इन और आईआरडीएआई को निर्धारित समय-सीमा के अंदर दी गई। यदि नहीं, तो इसके लिए कारण प्रस्तुत करें।
	कोई अन्य एजेंसी (नाम, तारीख लिखें):
क्या घटना की सूचना पुलिस को दी गई / एफआईआर फाइल की गईः	

घटना की सूचना	
क्या यह -	☐ नई घटना ☐ पिछली घटना के बारे में अद्यतन सूचना
घटना सर्वप्रथम कब पाई गई / कब देखी गई / इसकी पहचान कब की गई ? (तारीख और समय लिखें)	
घटना सर्वप्रथम कैसे पाई गई / इसकी पहचान की गई? (किसी अलार्म, चेतावनी, या जाँच को प्रेरित करनेवाली संदिग्ध गतिविधि को शामिल करें)	
घटना को किसने पाया? (नाम, विभाग और पदनाम लिखें) यदि किसी बाह्य संस्था के द्वारा पाई गई / सूचित की गई तो उसका नाम लिखें।	
घटना का प्रकार	☐ महत्वपूर्ण नेटवर्कों / प्रणाली का लक्ष्यित स्कैनिंग / जाँच ☐ महत्वपूर्ण प्रणालियों / सूचना का संकट ☐ आईटी प्रणालियों/डेटा में अनधिकृत प्रवेश

	☐ वेबसाइट का विरूपण या उसमें अनधिकृत प्रवेश ☐ दुर्भावपूर्ण कूट आक्रमण ☐ सर्वरों, जैसे डेटाबेस, मेल और डीएनएस तथा साधनों, जैसे राउटरों पर आक्रमण ☐ चोरी, स्पूफिंग और फ़िशिंग आक्रमण की पहचान ☐ डीओएस / डीडीओएस आक्रमण ☐ महत्वपूर्ण बुनियादी संरचना पर आक्रमण, एससीएडीए और परिचालनात्मक आक्रमण ☐ प्रौद्योगिकीगत प्रणालियाँ और बेतार नेटवर्क ☐ अनुप्रयोगों पर आक्रमण ☐ डेटा भंग ☐ डेटा प्रकटन ☐ वस्तुओं के इंटरनेट (आईओटी) साधनों, तथा संबद्ध प्रणालियों, नेटवर्कों, साफ्टवेयर, सर्वरों आदि पर आक्रमण ☐ दुर्भावपूर्ण अथवा जाली मोबाइल ऐपों के माध्यम से आक्रमण ☐ सोशल मीडिया खातों में अनधिकृत प्रवेश ☐ क्लाउड संगणना प्रणालियों / सर्वरों / साफ्टवेयर / अनुप्रयोगों को प्रभावित करनेवाले आक्रमण अथवा दुर्भावपूर्ण / संदिग्ध कार्यकलाप ☐ अन्य, विनिर्दिष्ट करें
क्या यह घटना पूर्व में सूचित की गई किसी अन्य घटना से संबंधित है? यदि “हाँ” तो दोनों घटनाएँ कैसे संबंधित हैं, इस पर अधिक सूचना प्रस्तुत करें।	
किस गंभीरता के रूप में यह घटना वर्गीकृत की जा रही है? (1 से 5 तक के मान पर, जहाँ 1 कम प्रभाव और 5 अत्यधिक प्रभाव से युक्त है)	
क्या प्रभावित प्रणाली(प्रणालियाँ) / नेटवर्क संस्था के लिए महत्वपूर्ण है/हैं?	
प्रभावित प्रणाली की मूलभूत जानकारी	क्षेत्र (डोमेन) / यूआरएलः
	आईपी पताः
	परिचालन प्रणालीः
	निर्माण (मेक) / माडल / क्लाउड विवरणः
	प्रभावित अनुप्रयोग विवरण (यदि कोई हो):
	प्रभावित प्रणाली का स्थान (नगर, क्षेत्र और देश सहित):
	क्या किसी ज्ञात असुरक्षितता का अनुचित लाभ उठाया गया हैः यदि हाँ, तो उसका पूरा विवरण प्रस्तुत करें:
	नेटवर्क और आईएसपी का नामः
	क्या कोई ज्ञात टीसीपी अथवा यूडीपी पोर्ट उक्त घटना में संबद्ध हैं :
	वर्तमान में प्रणाली पर संस्थापित सुरक्षा साफ्टवेयरः
	यदि ज्ञात हो, तो आक्रमणकर्ता का आईपी पता/ आईओसीएस प्रस्तुत करें :
क्या प्रभावित महत्वपूर्ण प्रणाली(लियों) / नेटवर्क (नेटवर्कों) का संस्था की किसी अन्य महत्वपूर्ण प्रणाली/महत्वपूर्ण आस्ति(यों) पर संभावित प्रभाव है?	

यदि “हाँ”, तो संभावित प्रभाव पर अधिक जानकारी प्रस्तुत करें।	
आक्रमण का प्रभाव क्या है? प्रत्येक पंक्ति के लिए एक पर निशान (टिक) लगाएँ।	संवेदनशील अथवा वैयक्तिक रूप से पता लगाई जा सकनेवाली सूचना (की हानि): ☐ कोई हानि नहीं ☐ अल्प हानि ☐ बड़ी हानि ☐ गंभीर हानि
	ग्राहक सेवा वितरण ☐ कोई हानि नहीं ☐ अल्प हानि ☐ बड़ी हानि ☐ गंभीर हानि
	जनता का विश्वास और प्रतिष्ठा ☐ कोई हानि नहीं ☐ अल्प हानि ☐ बड़ी हानि ☐ गंभीर हानि
घटनाओं का तैथिक क्रम	
घटना की तारीख, प्रारंभ का समय (लागों के अनुसार) और अवधिः	
घटना की प्रतिक्रिया प्रक्रिया का प्रबंध करने के लिए उत्तरदायी व्यक्ति का नाम (नाम, पदनाम, कार्यालयीन ई-मेल)	
घटना को कम करने के लिए अंतरिम उपायों पर की गई अनुमोदन की अपेक्षाओं सहित, किये गये उन्नयन, तथा ऐसे उपाय करने के लिए कारण	
हितधारकों को सूचित किया गया अथवा संबद्ध किया गया	
प्रयुक्त संचार के माध्यम (उदा. ई-मेल, इंटरनेट, एसएमएस, प्रेस प्रकाशनी, वेबसाइट सूचना, आदि)	
बीसीपी और / या डीआर के निर्णय / सक्रियण संबंधी तर्काधार	
घटना की स्थिति	
कौन-सी अनुवर्तन / सुधारात्मक कार्रवाइयाँ की गई हैं :	
इस घटना की वर्तमान स्थिति अथवा समाधान क्या है? यदि इसका समाधान नहीं किया गया है तो कार्रवाइयों का अगला क्रम क्या है?	
घटना का स्रोत / कारण क्या है? [(यदि मालूम नहीं है तो `उपलब्ध नहीं' (एनए)]	
क्या अभिरक्षा की शृंखला अनुरक्षित की जाती है?	
घटना से साक्ष्य का संग्रहण करने के लिए किन उपकरणों का उपयोग किया गया है?	
प्रथम सूचना देने के समय / अनुवर्ती सूचना देने	

के समय तक संस्था के द्वारा कौन-सी कार्रवाइयाँ अथवा प्रतिक्रियाएँ की गई हैं?	
क्या संस्था ने उक्त घटना से प्राप्त शिक्षा का अभिनिर्धारण किया है?	
मूल कारण संबंधी विश्लेषण	
घटना के घटित होने के लिए कारण क्या हैं? (घटना के लिए कारणभूत अथवा मार्ग प्रशस्त करनेवाले कारक)	
उक्त समस्या को कम करने / उसका समाधान करने के लिए अंतरिम उपाय, तथा ऐसे उपाय करने के लिए कारण।	
दीर्घकालिक परिप्रेक्ष्य के साथ समस्या का समाधान करने के लिए पहचाने गये या उठाये जानेवाले कदम। घटना के इसी प्रकार की भावी घटनाओं के घटित होने को रोकने के लिए की गई सुधारात्मक कार्रवाइयाँ।	
समाधान का दिनांक / लक्ष्यित दिनांक	
आक्रमण सदिश)अटैक वेक्टर्स(	
क्या संस्था ने उक्त घटना से संबंधित आईपी पतों, क्षेत्र (डोमेन) नामों की पहचान की है?	
समझौते के किन्हीं संकेतकों, पहचाने गये आईपी पतों की सूची और उनकी संबद्धता, समाधान किये गये क्षेत्रों के नामों, पहचाने गये ई-मेल पतों और उनकी संबद्धता, दुर्भावपूर्ण फाइलों/संलग्नकों (फाइल नाम, आकार, एमडी5/एसएचए1 हैश, आदि) आदि का उल्लेख करें।	

Basic Details	
Name of the entity	
Name of the person reporting	
Designation and Department	
Official email id	
Telephone / Mobile No.	
Provide Date and Time of Reporting incident to	IRDAI:
	CERT-In:
	Whether the reporting of incident to Cert-In & IRDAI was done within prescribed timeframe. If not, provide reasons thereof.
	Any other agency (mention name, date):
Whether incident reported to police / FIR filed:	
Incident Information	
Is this -	☐ New Incident ☐ Update about previous incident
When was the incident first observed/sighted/detected? (Provide Date and Time)	
How was the incident first observed/detected? (Include any alarms, alerts, or suspicious activity that triggered the investigation)	
Who observed the incident? (Provide Name, Department & Designation) In case it was observed / informed by external entity, please mention name of the same.	
Type of incident	☐ Targeted scanning/probing of critical networks/systems ☐ Compromise of critical systems/information ☐ Unauthorized access of IT systems/data ☐ Defacement or intrusion into the website ☐ Malicious code attacks ☐ Attack on servers such as Database, Mail and DNS and network devices such as Routers ☐ Identity Theft, spoofing and phishing attacks ☐ DoS/DDoS attacks ☐ Attacks on Critical infrastructure, SCADA and operational technology systems and wireless networks ☐ Attacks on Applications ☐ Data Breach ☐ Data Leak ☐ Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers etc. ☐ Attacks through malicious or fake Mobile Apps

	☐ Unauthorised access to social media accounts ☐ Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications ☐ Others, please specify:
Is this incident related to another incident previously reported? If "Yes", provide more information on how both incidents are related.	
What severity is this incident being classified as? (On a scale of 1 to 5, with 1 being low impact and 5 being high impact)	
Is the affected system(s) / network(s) critical to the entity?	
Basic information of affected system	Domain/URL:
	IP Address:
	Operating System:
	Make/Model/Cloud details:
	Affected Application details (If any):
	Location of affected system (including City, Region & Country):
	Whether any known vulnerability was exploited: If yes, please provide complete details of the same:
	Network and name of ISP:
	Any known TCP or UDP ports involved in the incident:
	Security software installed on the system currently:
	If known, provide the attacker's IP address/ IOCs:
Does the affected critical system(s) / network(s) have potential impact on another critical system / critical asset(s) of the entity? If "Yes", provide more information on potential impact.	
What is the impact of the attack? Tick one for each row.	(Loss of) Sensitive or Personally Identifiable Information: ☐ No Loss ☐ Minor Loss ☐ Major Loss ☐ Severe Loss
	Customer Service Delivery ☐ No Loss ☐ Minor Loss ☐ Major Loss ☐ Severe Loss
	Public Confidence and Reputation ☐ No Loss ☐ Minor Loss ☐ Major Loss ☐ Severe Loss

Chronological order of events	
Date of incident, start time (as per the logs) and duration:	
Details of person responsible for managing the incident response process (Name, Designation, Official email)	
Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
Stakeholders informed or involved	
Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
Rationale on the decision / activation of BCP and / or DR	
Incident Status	
What are the follow up / corrective actions that have been:	
What is the current status or resolution of this incident? If it is not resolved, what is the next course of actions?	
What is the source/cause of the incident? ('NA' if unknown)	
Is chain of custody maintained?	
What tools were used for collecting the evidence for the incident?	
What actions or responses have been taken by the entity at the time of first reporting/till the time of subsequent reporting?	
Has the entity identified key lessons learned from the incident?	
Root Cause Analysis	
What are the reasons for the occurrence of the incident? (Factors that caused or lead to the incident)	
Interim measures to mitigate / resolve the issue, and reasons for taking such measures.	
Steps identified or to be taken to address the issue with the long term perspective. Corrective actions taken to prevent future occurrences of similar types of incident.	
Date / target date of resolution	
Attack Vectors	

Did the entity identify IP addresses, domain names, related to the incident?	
Mention any Indicators of Compromise, list of IP addresses identified and their involvement, domain names resolved, email addresses identified and their involvement, malicious files / attachments (file name, size, MD5/SHA1 hash, etc.), etc.	