**Name of Organization**

**Incident Response Acronyms**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Acronyms

The (Name of Organization) Incident Response Acronyms document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need to know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

## Table 1: Acronyms

|  |  |
| --- | --- |
| **Category** | **Description** |
| 2FA | **Two-Factor Authentication** |
| AA | **After Action** |
| AHJ | **Authority Having Jurisdiction** |
| APWG | **Anti-Phishing Working Group** |
| BAL | **Business Alignment Leaders** |
| BC | **Business Continuity** |
| BCBS | **Basel Committee on Banking Supervision** |
| BCP | **Business Continuity Plan** |
| BIA | **Business Impact Analysis** |
| CCIPS | **Computer Crime and Intellectual Property Section** |
| CCPA | **Consumer Credit Protection Act** |
| CFR | **Code of Federal Regulations** |
| CFTC | **Commodity Futures Trading Commission** |
| CIO | **Chief Information Officer** |
| CIRT | **Cybersecurity Incident Response Team** |
| CISO | **Chief Information Security Officer** |
| COG | **Continuity of Government** |
| COOP | **Continuity of Operations** |
| CSD | **Computer Security Division** |
| CSF | **Cyber Security Framework** |
| CSIRT | **Cyber Security Incident Response Team** |
| CTO | **Chief Technology Officer** |
| DDoS | **Distributed Denial of Service** |
| DHS | **U.S. Department of Homeland Security** |
| DIR | **Texas Department of Information Resources** |
| DOI | **Digital Object Identifier** |
| DoS | **Denial of Service** |
| DPO | **Data Privacy Officer** |
| DR | **Disaster Recovery** |
| DRP | **Disaster Recovery Plan** |
| EAT | **Export Address Table** |
| EFA | **Expedited Funds Availability** |
| EISO | **Enterprise Information Security Office** |
| EMA | **Emergency Management Agency** |
| EMAC | **Emergency Management Assistance Compact** |
| EMI | **Emergency Management Institute** |
| ENISA | **European Network and Information Security Agency** |
| EOC | **Emergency Operations Center** |
| ESF | **Emergency Support Function** |
| FBI | **Federal Bureau of Investigation** |
| FDA | **Food and Drug Administration** |
| FEMA | **Federal Emergency Management Agency** |
| FFIEC | **Federal Financial Institutions Examination Council** |
| FIL | **Financial Institution Letter** |
| FINRA | **Financial Industry Regulatory Authority** |
| FIPS PUB 199 | **Federal Information Processing Standard Publication 199** |
| FIRST | **Forum of Incident Response and Security Teams** |
| FISMA | **Federal Information Security Modernization Act** |
| FOUO | **For Official Use Only** |
| FPM | **Final Planning Meeting** |
| FRPG | **Federal Response Planning Guidance** |
| GASB | **Governmental Accounting Standards Board** |
| GDPR | **General Data Protection Regulation** |
| GFIRST | **Government Forum of Incident Response and Security Teams** |
| GLBA | **Gramm-Leach-Bliley Act** |
| HA | **High Availability** |
| HIPAA | **Health Insurance Portability and Accountability Act** |
| HTCIA | **High Technology Crime Investigation Association** |
| IANA | **Internet Assigned Numbers Authority** |
| IAP | **Incident Action Plan** |
| IAT | **Import Address Table** |
| IC | **Incident Commander** |
| ICS | **Incident Command Systems** |
| IDPS | **Intrusion Detection and Prevention System** |
| IDS | **Intrusion Detection System** |
| IEC | **International Electrotechnical Commission** |
| IHT | **Incident Handling Team** |
| IMCM | **Incident Management Capability Metrics** |
| IO | **Information Officer** |
| IoC | **Indicators of Compromise** |
| IPM | **Initial Planning Meeting** |
| IPS | **Intrusion Protection System** |
| IR | **Incident Response** |
| IRP | **Incident Response Plan** |
| IRS | **Internal Revenue Service** |
| ISAC | **Information Sharing and Analysis Centers** |
| ISC | **Internet Store Center** |
| ISCP | **Information System Contingency Plan** |
| ISO | **International Organization for Standardization** |
| ISP | **Internet Service Provider** |
| ISR | **Incident Summary Report** |
| IT | **Information Technology** |
| ITDRP | **Information Technology Disaster Recovery Plan** |
| JIC | **Joint Information Center** |
| LDAP | **Lightweight Directory Access Protocol** |
| MAC | **Multiagency Cooperation Group** |
| MACS | **Multi-Agency Coordination System** |
| MFT | **Master File Table** |
| MOA | **Memorandum of Agreement** |
| MOU | **Memorandum of Understanding** |
| MRD-IMC | **Mission Risk Diagnostic for Incident Management Capabilities** |
| MSP | **Major Swap Participant** |
| MTD | **Maximum Tolerable Downtime** |
| NASD | **National Association of Securities Dealers** |
| NCSR | **Nationwide Cybersecurity Review** |
| NDA | **Nondisclosure Agreement** |
| NDCA | **National Defense Cyber Alliance** |
| NERC CIP | **North American Electric Reliability Corporation Critical Infrastructure Protection** |
| NIC | **National Integration Center** |
| NICCL | **National Incident Communications Conference Line** |
| NIMS | **National Incident Management System** |
| NIST | **National Institute of Standards and Technology** |
| NQS | **National Qualification System** |
| NTP | **Network Time Protocol** |
| NYSE | **New York Stock Exchange** |
| OCC | **Office of the Comptroller of the Currency** |
| OEM | **Office of Emergency Management** |
| OEP | **Occupant Emergency Plan** |
| Opsi | **Open PC Server Integration** |
| OSSIM | **Open-Source Security Information Management** |
| P1 | **Priority Level 1/High** |
| P2 | **Priority Level 2/Moderate** |
| P3 | **Priority Level 3/Low** |
| PCAP | **Packet Captures** |
| PCI | **Payment Card Industry** |
| PCI DSS | **Payment Card Industry Data Security Standard** |
| PICCL | **Private Sector Incident Communications Conference Line** |
| PII | **Personally Identifiable Information** |
| PIO | **Public Information Officer** |
| PIP | **Process Improvement Plan** |
| POC | **Point of Contact** |
| PPE | **Personal Protective Equipment** |
| PPT | **People, Process, and Technology** |
| RPO | **Recovery Point Objective** |
| RTO | **Recovery Time Objective** |
| SD | **Swap Dealer** |
| SE | **Security Engineer** |
| SEC | **Securities and Exchange Commission** |
| SICCL | **State Incident Communications Conference Line** |
| SIEM | **Security Information and Event Management** |
| SIFT | **SANS Investigative Forensics Toolkit** |
| SIM3 | **Security Incident Management Maturity Model** |
| SitMan | **Situation Manual** |
| SLA | **Service Level Agreements** |
| SLTT | **State, Local, Tribal & Territorial** |
| SME | **Subject Matter Expert** |
| SOP | **Standard Operating Procedures** |
| SOX | **Sarbanes-Oxley Act** |
| SPI | **Sensitive Personal Information** |
| SSDT | **SQL Server Data Tools** |
| SSP | **System Security Plan** |
| TCP | **Transmission Control Protocol** |
| TDoS | **Telephony Denial of Service** |
| TPRM | **Third-Party Risk Management** |
| TTX | **Table Top Exercise** |
| UAC | **Unix-like Artifacts Collector** |
| US-CERT | **United States Computer Emergency Readiness Team** |
| VM | **Virtual Machine** |
| VPN | **Virtual Private Network** |
| XDR | **Extended Detection and Response** |