LEXCLAW

Jurisdiction Cybersecurity Law Report

Global (GLOBAL)
Generated: March 17, 2026

Summary

50
Total Laws & Regulations

48
Currently In Force

Cybersecurity Laws & Regulations

Law / Regulation	Status	Effective Date	Sector
SOCI Act Security of Critical Infrastructure Act 2018	In Force	2018-07-11	critical infrastructure
SOCI Act 2022 (Australia) Security of Critical Infrastructure Act 2018 (SOCI) — 2022 Amendments	In Force	2022-04-02	Energy, Water, Transport, Finance, Healthcare, Food, Education, Space, Defence industry, Communications, Data storage and processing
BACEN 4893 (Brazil) BACEN Resolution 4893/2021 — Cybersecurity Policy for Financial Institutions	In Force	2021-02-26	Banking, Financial institutions, Payment institutions
ANPD Incident Reporting (Brazil) ANPD Resolution CD/ANPD No. 2/2022 — Security Incident Reporting	In Force	2022-05-27	All sectors processing personal data
BACEN Resolution 4893 Resolução CMN nº 4.893/2021 — Cybersecurity Policy for Financial Institutions	In Force	2022-12-31	financial
Directive on Security Management (Canada) Treasury Board Directive on Security Management	In Force	2019-07-01	Federal government departments and agencies
Bill C-26 / CCSPA (Canada) Bill C-26 — An Act Respecting Cyber Security (Critical Cyber Systems Protection Act)	Proposed	N/A	Finance, Telecommunications, Energy, Transportation, Nuclear

Law / Regulation	Status	Effective Date	Sector
CSL (China) Cybersecurity Law of the People's Republic of China	In Force	2017-06-01	All sectors, Critical information infrastructure, Network operators
China Cybersecurity Law Cybersecurity Law of the People's Republic of China	amended	2017-06-01	cross-sector
CII Regulations (China) Critical Information Infrastructure Security Protection Regulations	In Force	2021-09-01	Energy, Finance, Transportation, Water, Healthcare, Government, Telecommunications
DSL (China) Data Security Law of the People's Republic of China	In Force	2021-09-01	All sectors, Data processors, Critical information infrastructure
Cyber Resilience Act (CRA) Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act)	In Force	2024-12-11	technology
NIS2 Directive Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2)	In Force	2024-10-17	cross-sector
DORA Digital Operational Resilience Act	In Force	2025-01-17	financial
LPM 2024 (France) Military Programming Law 2024-2030 (LPM) — Cybersecurity Provisions	In Force	2023-08-01	Defense, Critical infrastructure, Essential services, Government
IT-SiG 2.0 (Germany) IT Security Act 2.0 (BSI-Gesetz / BSIG Amendment)	In Force	2021-05-28	Critical infrastructure, Energy, Water, Finance, Healthcare, Transport, Digital infrastructure
Ghana NCPS 2021 National Cybersecurity Policy and Strategy	In Force	2021-06-01	cross_sector
Ghana Cybersecurity Act 2020 Cybersecurity Act	In Force	2020-12-29	cross_sector
HKMA CFI 2.0 (Hong Kong) HKMA Cybersecurity Fortification Initiative 2.0 (CFI 2.0)	In Force	2021-11-01	Banking, Financial institutions, Authorized institutions
CERT-In Directions 2022 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 — CERT-In Cybersecurity Directions 2022	In Force	2022-06-28	cross-sector
IT Act S.43A (India) Information Technology Act 2000 — Section 43A (Reasonable Security Practices)	In Force	2008-10-27	All sectors handling sensitive personal data
RBI IT Framework (India) RBI Master Direction on Information Technology Framework for Banks	In Force	2016-06-02	Banking, Scheduled commercial banks, Urban cooperative banks

Law / Regulation	Status	Effective Date	Sector
INCD Directive 2.0 (Israel) INCD Directive 2.0 — Cybersecurity Protection of Critical Infrastructure	In Force	2021-01-01	Energy, Water, Finance, Healthcare, Transportation, Defense industry, Government, Telecommunications
UCPA (Japan) Act on Prohibition of Unauthorized Computer Access	In Force	2000-02-13	All sectors
Cybersecurity Basic Act (Japan) Basic Act on Cybersecurity (Cybersecurity Basic Act)	In Force	2015-01-09	Government, Critical infrastructure, All sectors
SDS Act (Japan) Act on Protection of Specially Designated Secrets	In Force	2014-12-10	Defense, Government, Defense contractors
Kenya NCS 2022 National Cybersecurity Strategy 2022–2027	In Force	2022-01-01	cross_sector
Kenya CMCA 2018 Computer Misuse and Cybercrimes Act	In Force	2018-05-30	cross_sector
CNBV CUB Cybersecurity (Mexico) CNBV Circular Única de Bancos — Cybersecurity Requirements	In Force	2021-01-01	Banking institutions, Financial entities
Wbni / NIS2 (Netherlands) Network and Information Systems Security Act (Wbni) — NIS2 Implementation	In Force	2018-11-09	Energy, Transport, Banking, Financial market infrastructure, Healthcare, Drinking water, Digital infrastructure, ICT service management
23 NYCRR Part 500 NYDFS Cybersecurity Regulation	In Force	2023-11-01	financial
TICSA (New Zealand) Telecommunications (Interception Capability and Security) Act 2013 (TICSA)	In Force	2013-11-01	Telecommunications, Network operators, Internet service providers
Nigeria Cybercrimes Act Cybercrimes (Prohibition, Prevention, etc.) Act	In Force	2015-05-15	cross_sector
NCA CCC (Saudi Arabia) NCA Cloud Computing Cybersecurity Controls (CCC-1:2020)	In Force	2020-01-01	Government entities, Critical national infrastructure, Cloud service providers
NCA ECC Essential Cybersecurity Controls (ECC)	In Force	2018-01-01	cross-sector
SAMA CSF (Saudi Arabia) SAMA Cybersecurity Framework	In Force	2017-05-01	Banking, Insurance, Financial market institutions, Payment services
Singapore Cybersecurity Act Cybersecurity Act 2018 (as amended by Cybersecurity (Amendment) Act 2024)	In Force	2018-08-31	cross-sector
CSA CCoP (Singapore) CSA Cybersecurity Code of Practice for Critical Information Infrastructure	In Force	2022-07-04	Energy, Water, Banking, Finance, Healthcare, Transport, Infocomm, Media, Security and emergency services, Government, Aviation
MAS TRM Guidelines (Singapore) MAS Technology Risk Management Guidelines	In Force	2021-01-18	Banking, Insurance, Capital markets, Payment services

Law / Regulation	Status	Effective Date	Sector
Cybercrimes Act (South Africa) Cybercrimes Act 19 of 2020	In Force	2021-12-01	All sectors, Electronic communications service providers
South Africa Cybercrimes Act Cybercrimes Act 19 of 2020	In Force	2021-12-01	cross-sector
POPIA Cybersecurity (South Africa) Protection of Personal Information Act 4 of 2013 — Cybersecurity Obligations (POPIA)	In Force	2021-07-01	All sectors processing personal information
ICN Act (South Korea) Act on Information and Communications Network Utilization and Information Protection	In Force	2001-07-01	ICT service providers, E-commerce, Financial services, Healthcare
PICI Act (South Korea) Act on the Protection of Information and Communications Infrastructure	In Force	2001-07-01	Critical information infrastructure, Government, Finance, Energy, Telecommunications
ISG (Switzerland) Federal Act on Information Security in the Confederation (ISG)	In Force	2023-01-01	Government, Critical infrastructure
CBUAE Cyber Framework (UAE) CBUAE Cybersecurity Framework for Financial Institutions	In Force	2021-01-01	Banking, Insurance, Financial services, Payment services
NESA IAS (UAE) NESA Information Assurance Standards (IAS)	In Force	2014-01-01	Critical national infrastructure, Government, Energy, Finance, Telecommunications
UAE Cybercrime Law Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime	In Force	2022-01-02	cross-sector
UK NIS Regulations Network and Information Systems (NIS) Regulations 2018	In Force	2018-05-10	cross-sector
PSTI Act Product Security and Telecommunications Infrastructure Act 2022	In Force	2024-04-29	technology

SOCI Act

The SOCI Act protects Australia's critical infrastructure from cybersecurity and other risks. It was significantly expanded in 2022 to cover 11 sectors and introduce mandatory risk management programs and enhanced incident reporting. It requires responsible entities to register assets, report incidents, and implement risk management programs.

Official Source: https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

SOCI Act 2022 (Australia)

Significantly expanded Australia's critical infrastructure security framework. Extended to 11 sectors, introduced positive security obligations, mandatory incident reporting within 12 hours for critical incidents, government assistance powers, and enhanced cybersecurity obligations for systems of national significance.

Official Source: https://www.cisc.gov.au/

BACEN 4893 (Brazil)

Brazil's Central Bank resolution requiring financial institutions to establish comprehensive cybersecurity policies, conduct annual risk assessments, implement security controls, and report significant cyber incidents. Requires board-level approval of cybersecurity policies.

Official Source: https://www.bcb.gov.br/

ANPD Incident Reporting (Brazil)

Establishes the framework for reporting personal data security incidents under Brazil's LGPD. Requires controllers to notify ANPD and affected data subjects within 72 hours of becoming aware of incidents that may cause significant harm.

Official Source: https://www.gov.br/anpd/

BACEN Resolution 4893

BACEN Resolution 4893 requires Brazilian financial institutions to implement a cybersecurity policy, conduct annual risk assessments, manage third-party risks, and report significant incidents to the central bank.

Official Source: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893

Directive on Security Management (Canada)

Governs security management across the Government of Canada. Requires departments to implement security programs covering personnel, physical, IT, and information security. Mandates security assessments, incident reporting, and business continuity planning.

Official Source: https://www.tbs-sct.canada.ca/

Bill C-26 / CCSPA (Canada)

Proposed Canadian legislation to protect critical cyber systems in federally regulated sectors. Would require designated operators in finance, telecommunications, energy, and transportation to establish cybersecurity programs, report incidents, and comply with government cybersecurity directions.

Official Source: https://www.publicsafety.gc.ca/

CSL (China)

China's foundational cybersecurity law establishing obligations for network operators, critical information infrastructure (CII) operators, and data handlers. Requires data localization for CII operators, network security reviews, and real-name registration.

Official Source: http://www.cac.gov.cn/

China Cybersecurity Law

China's Cybersecurity Law is the foundational cybersecurity statute, establishing obligations for network operators and critical information infrastructure operators. It requires real-name registration, data localization for CII, security reviews for CII procurement, and incident reporting. The law was significantly amended in January 2026, with enhanced enforcement powers and increased penalties.

Official Source: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

CII Regulations (China)

Detailed regulations for protecting China's critical information infrastructure in sectors including energy, finance, transportation, water, healthcare, and government. Mandates security assessments, personnel background checks, and procurement security reviews.

Official Source: http://www.gov.cn/

DSL (China)

Establishes a data classification and grading system based on national security importance. Requires organizations to implement data security management systems, conduct risk assessments, and report security incidents. Restricts cross-border data transfers.

Official Source: http://www.cac.gov.cn/

Cyber Resilience Act (CRA)

The CRA is the EU's first horizontal cybersecurity law for products with digital elements — covering everything from smart devices to software. It requires manufacturers to build security in by design, maintain security throughout the product lifecycle, report vulnerabilities, and provide security updates. It entered into force in December 2024, with most obligations applying from December 2027.

Official Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

NIS2 Directive

NIS2 is the EU's updated network and information security directive, replacing NIS1. It significantly expands the scope of covered entities, strengthens cybersecurity requirements, and increases penalties. It applies to medium and large enterprises in 18 critical sectors. Member states were required to transpose it into national law by October 17, 2024. It introduces management liability for cybersecurity failures and requires 24-hour early warning and 72-hour notification for significant incidents.

Official Source: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

DORA

DORA is an EU regulation that applies directly to financial entities and their ICT service providers. It creates a comprehensive framework for digital operational resilience including ICT risk management, incident reporting, resilience testing, and third-party risk management. It became applicable on January 17, 2025. Unlike NIS2, DORA is a regulation (directly applicable) rather than a directive, so it does not require national transposition.

Official Source: https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act

LPM 2024 (France)

France's Military Programming Law 2024-2030 includes significant cybersecurity provisions expanding ANSSI's authority, mandating incident reporting for operators of vital importance (OIV) and essential services (OSE), and implementing NIS2 transposition requirements.

Official Source: https://www.ssi.gouv.fr/

IT-SiG 2.0 (Germany)

Germany's expanded IT security law strengthening the Federal Office for Information Security (BSI). Extends KRITIS (critical infrastructure) obligations to additional sectors, introduces mandatory use of attack detection systems, and grants BSI new investigative powers.

Official Source: https://www.bsi.bund.de/

Ghana NCPS 2021

Ghana's strategic framework for implementing the Cybersecurity Act 2020. Establishes seven strategic pillars: Legal and Regulatory Framework; Technical Measures and Standards; Organisational Structures; Capacity Building; International Cooperation; Child Online Protection; and Cybersecurity Culture. Designates 11 critical information infrastructure sectors and establishes baseline security requirements for each.

Official Source: https://www.csa.gov.gh/assets/docs/National-Cybersecurity-Policy-Strategy-2021.pdf

Ghana Cybersecurity Act 2020

Ghana's comprehensive cybersecurity statute establishing the Cyber Security Authority (CSA) as the national cybersecurity regulator. Creates a national cybersecurity framework, designates and protects critical information infrastructure, establishes incident reporting requirements, and creates a licensing framework for cybersecurity service providers. One of Africa's most comprehensive standalone cybersecurity laws.

Official Source: https://www.csa.gov.gh/assets/docs/Cybersecurity-Act-2020-Act-1038.pdf

HKMA CFI 2.0 (Hong Kong)

Hong Kong Monetary Authority's updated cybersecurity framework for authorized institutions. Requires cyber maturity assessments, penetration testing, cyber intelligence sharing, and incident reporting. Introduces a Cyber Intelligence Sharing Platform (CISP) for financial institutions.

Official Source: https://www.hkma.gov.hk/

CERT-In Directions 2022

The CERT-In Directions 2022 require all entities in India to report cybersecurity incidents to CERT-In within 6 hours — one of the shortest mandatory reporting windows globally. They also require 180-day log retention, NTP synchronization, and 5-year record retention for VPN providers, cloud service providers, and virtual asset service providers.

Official Source: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

IT Act S.43A (India)

Section 43A of India's IT Act requires body corporates handling sensitive personal data to implement reasonable security practices and procedures. Failure to do so resulting in wrongful loss or gain creates civil liability for compensation.

Official Source: https://www.meity.gov.in/

RBI IT Framework (India)

Reserve Bank of India's comprehensive IT governance and cybersecurity framework for banks. Mandates IT governance structures, cybersecurity policies, incident reporting, business continuity, and third-party risk management. Requires a Chief Information Security Officer (CISO).

Official Source: https://www.rbi.org.in/

INCD Directive 2.0 (Israel)

Israel's National Cyber Directorate directive establishing cybersecurity requirements for critical infrastructure operators. Mandates security controls, incident reporting within 12 hours, annual assessments, and supply chain security for 19 critical infrastructure sectors.

Official Source: https://www.gov.il/en/departments/incd

UCPA (Japan)

Japan's primary law prohibiting unauthorized access to computer systems. Criminalizes unauthorized login, phishing, and credential theft. Penalties include up to 3 years imprisonment or fines up to ¥1 million.

Official Source: https://www.nisc.go.jp/eng/

Cybersecurity Basic Act (Japan)

Establishes Japan's national cybersecurity policy framework. Creates the National center of Incident readiness and Strategy for Cybersecurity (NISC) and mandates cybersecurity strategies for critical infrastructure operators.

Official Source: https://www.nisc.go.jp/eng/

SDS Act (Japan)

Governs the protection of specially designated secrets in defense, diplomacy, counterterrorism, and counterintelligence. Imposes strict security clearance requirements and cybersecurity obligations for handling classified information.

Official Source: https://www.nisc.go.jp/eng/

Kenya NCS 2022

Kenya's strategic framework for building a secure, resilient, and trusted cyberspace through 2027. Built around five pillars: Cybersecurity Governance; Legislation and Regulation; Capacity Building; Culture and Awareness; and International Cooperation. Designates the National KE-CIRT/CC as the national coordination centre and establishes sector-specific requirements for critical infrastructure.

Official Source: https://www.icta.go.ke/wp-content/uploads/2022/09/National-Cybersecurity-Strategy-2022-2027.pdf

Kenya CMCA 2018

Kenya's principal legislation addressing cybercrime and cybersecurity. Establishes offences relating to unauthorised access, computer fraud, cyber espionage, and critical infrastructure attacks. Grants law enforcement powers including production orders and real-time interception. Establishes the National Computer and Cybercrimes Coordination Committee (NC4). Partially suspended by the High Court in 2018 on freedom of expression grounds, with certain provisions subsequently reinstated.

Official Source:
https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2018/TheComputerMisuseandCybercrimesAct_No5of2018.pdf

CNBV CUB Cybersecurity (Mexico)

Mexico's banking regulator (CNBV) requirements for cybersecurity in banking institutions. Mandates information security management systems, incident response plans, business continuity, and reporting of significant cyber incidents to CNBV within 24 hours.

Official Source: https://www.cnbv.gob.mx/

Wbni / NIS2 (Netherlands)

Netherlands' implementation of EU NIS and NIS2 Directives. Requires essential and important entities to implement risk-based security measures, report significant incidents to NCSC within 24 hours, and register with competent authorities.

Official Source: https://www.ncsc.nl/

23 NYCRR Part 500

NYDFS Part 500 is one of the most comprehensive state-level cybersecurity regulations in the US. It applies to all financial services companies licensed in New York and requires a risk-based cybersecurity program, a CISO, MFA, encryption, penetration testing, and annual certification. The 2023 Second Amendment added new requirements for Class A companies (500+ employees or $10B+ revenue) including enhanced controls, independent audits, and additional technical safeguards.

Official Source: https://www.dfs.ny.gov/industry_guidance/cybersecurity

TICSA (New Zealand)

New Zealand law requiring telecommunications network operators to maintain interception capability and implement network security measures. Operators must notify GCSB of network changes that could affect security, and work with NCSC on cybersecurity incidents.

Official Source: https://www.ncsc.govt.nz/

Nigeria Cybercrimes Act

Nigeria's primary federal legislation governing cybercrime and cybersecurity. Criminalises unauthorised access, system interference, cyberstalking, identity theft, and cyber terrorism. Establishes obligations for critical national information infrastructure operators and creates a Cybercrime Fund financed by levies on electronic transactions. Amended in 2024 to address cyberbullying.

Official Source:
https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

NCA CCC (Saudi Arabia)

Saudi National Cybersecurity Authority controls for cloud computing security. Mandatory for government entities and critical national infrastructure using cloud services. Establishes 4 domains of cloud security controls covering governance, compliance, data protection, and operational security.

Official Source: https://www.nca.gov.sa/

NCA ECC

The NCA Essential Cybersecurity Controls establish 114 mandatory cybersecurity controls for Saudi government entities and organizations of national importance. They cover governance, defense, resilience, third-party risk, industrial control systems, and cryptography.

Official Source: https://nca.gov.sa/en/pages/ECC

SAMA CSF (Saudi Arabia)

Saudi Arabia Monetary Authority's cybersecurity framework for financial institutions. Based on international standards including NIST CSF and ISO 27001, it mandates cybersecurity governance, risk management, security controls, and incident response for banks, insurance companies, and financial market institutions.

Official Source: https://www.sama.gov.sa/

Singapore Cybersecurity Act

Singapore's Cybersecurity Act establishes the legal framework for protecting critical information infrastructure and regulating cybersecurity service providers. The 2024 amendments expanded the Act to cover systems of temporary cybersecurity concern, major cybersecurity incidents, and providers of foundational digital infrastructure services.

Official Source: https://www.csa.gov.sg/legislation/cybersecurity-act/

CSA CCoP (Singapore)

Mandatory code of practice under Singapore's Cybersecurity Act for Critical Information Infrastructure (CII) owners. Establishes cybersecurity risk management, incident reporting, and audit requirements for 11 CII sectors.

Official Source: https://www.csa.gov.sg/

MAS TRM Guidelines (Singapore)

Monetary Authority of Singapore's guidelines for technology risk management in financial institutions. Covers IT governance, cyber resilience, system availability, data management, and third-party risk. Requires incident reporting within 1 hour for significant disruptions.

Official Source: https://www.mas.gov.sg/

Cybercrimes Act (South Africa)

South Africa's comprehensive cybercrime law criminalizing unauthorized access, data interception, cyber fraud, and malicious communications. Requires electronic communications service providers to report cybercrime to SAPS within 72 hours and preserve evidence.

Official Source: https://www.justice.gov.za/

South Africa Cybercrimes Act

South Africa's Cybercrimes Act criminalizes cybercrimes and requires electronic communications service providers and financial institutions to report cybercrimes to SAPS within 72 hours. It also establishes obligations for evidence preservation and cooperation with investigations.

Official Source: https://www.justice.gov.za/legislation/acts/2020-019-cybercrimesact.pdf

POPIA Cybersecurity (South Africa)

POPIA's cybersecurity obligations require responsible parties to implement appropriate, reasonable technical and organizational measures to prevent loss, damage, or unauthorized access to personal information. Security breaches must be reported to the Information Regulator and affected data subjects.

Official Source: https://www.justice.gov.za/inforeg/

ICN Act (South Korea)

South Korea's primary law governing cybersecurity for information and communications networks. Requires information security management systems (ISMS), mandates incident reporting, prohibits unauthorized access, and regulates spam and malicious code.

Official Source: https://www.msit.go.kr/

PICI Act (South Korea)

Establishes the framework for protecting South Korea's critical information and communications infrastructure. Designates critical infrastructure, mandates security plans, requires annual vulnerability assessments, and establishes incident response procedures.

Official Source: https://www.msit.go.kr/

ISG (Switzerland)

Switzerland's federal information security law establishing uniform security requirements for federal authorities. Mandates information classification, security assessments, incident reporting to NCSC.

Official Source: https://www.bk.admin.ch/

CBUAE Cyber Framework (UAE)

Central Bank of UAE cybersecurity framework requiring licensed financial institutions to implement comprehensive cybersecurity programs. Mandates cyber risk governance, security controls, incident response, and third-party risk management aligned with international standards.

Official Source: https://www.centralbank.ae/

NESA IAS (UAE)

UAE's National Electronic Security Authority information assurance standards for critical national infrastructure. Establishes mandatory security controls across 18 domains for CNI operators, requiring annual compliance assessments and incident reporting.

Official Source: https://www.nesa.ae/

UAE Cybercrime Law

The UAE Cybercrime Law criminalizes unauthorized access to information systems, data breaches, electronic fraud, and cyberattacks. It applies to anyone committing cybercrimes in the UAE or targeting UAE systems from abroad. Organizations must implement security measures to prevent unauthorized access.

Official Source: https://uaelegislation.gov.ae/en/legislations/1972

UK NIS Regulations

The UK NIS Regulations 2018 implemented the EU's original NIS Directive into UK law before Brexit. They require operators of essential services and digital service providers to implement appropriate security measures and report significant incidents. The UK is now developing the Cyber Security and Resilience Bill to replace and strengthen these regulations.

Official Source: https://www.legislation.gov.uk/uksi/2018/506/contents

PSTI Act

The PSTI Act requires manufacturers of consumer IoT devices sold in the UK to meet basic security requirements: no default passwords, a published vulnerability disclosure policy, and transparency about security update support periods. It came into force in April 2024.

Official Source: https://www.gov.uk/guidance/product-security-and-telecommunications-infrastructure-psti-act-2022