GSMA

Policy Principles for Mobile Network Resilience

November 2026



Copyright © 2026 GSMA

GSMA™

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

The context: Resilience is a public policy priority

During crises and disruption – whether caused by extreme weather and natural disasters, geopolitical events or conflict – mobile networks keep people and communities connected. They enable access to essential services, support the coordination of relief efforts, and allow potentially life-saving information to be shared with relevant agencies. As society becomes increasingly reliant on uninterrupted connectivity, mobile network resilience is central to national preparedness, consumer protection and critical infrastructure policy, making it a shared priority for the mobile industry, governments and regulators worldwide.

Resilience refers to the capability and capacity of a network to maintain and/or recover its ability to deliver mobile services to users in the face of disruptive scenarios. This involves redundancy, diversity, robustness, recovery processes, and the ability to enhance and adapt infrastructure, people, and processes so that essential services continue to function - or are restored quickly - when disrupted. It also means learning from incidents and adapting to improve future performance. It depends on continually strengthening robust network designs and operational readiness, upskilling staff, further securing supply chains, backup power, diverse connectivity routes, rapid restoration processes and more effective coordination with government and other critical sectors.

The challenge: Risk is rising, but regulation is fragmented

The threats facing mobile networks are diverse and increasingly interconnected. Power disruption, vandalism and theft, physical security risks and geopolitical instability, natural disasters (earthquakes, flooding and storms), and dependency on other sectors can all affect the availability and continuity of mobile services. These risks do not sit neatly within one regulatory framework, or one sector. Instead, they cut across telecoms, energy, transport, emergency services, security, planning and local government. This creates a clear policy challenge. While operators already do a great deal, governments want enhanced resilience. Regulatory frameworks need to be designed carefully so that they support, rather than constrain, effective resilience investment and operational responses. Overlapping duties, inconsistent definitions, duplicate reporting, short implementation timelines and prescriptive technical mandates can divert investment and operational effort away from the measures most likely to keep citizens connected.

Where mobile networks are designated as critical infrastructure, legal, regulatory and voluntary frameworks can support resilience in different - and sometimes conflicting – ways. Telecoms and critical-infrastructure requirements typically address service continuity, public safety, emergency communications and incident reporting. In markets with climate-disclosure regimes, operators may also assess longer-term physical risks and their potential financial impact, influencing network design and operations. Voluntary frameworks allow operators to act on risk assessments, but poor alignment between these approaches and fragmented regulation can create confusion, legal and regulatory uncertainty and delay deployment of critical infrastructure. For example, in Europe, operators must comply with both the European Electronic Communications Code (EECC), which sets risk management, business continuity and incident reporting obligations, and the Critical Entities Resilience (CER) Directive, which imposes separate physical and hybrid resilience requirements. These are two overlapping regimes with inconsistent definitions and timescales that divide operators' efforts between improving resilience and demonstrating compliance.

Regulatory approaches also vary by geography. In parts of Africa, unstable power grids and resilience requirements often means prioritising backup power and fuel. In North America, Chile and Japan, operators are increasingly expected to incorporate roaming arrangements into disaster management systems. In Latin America, persistent theft and vandalism force operators to repeatedly replace equipment such as batteries, increasing costs without improving service continuity or achieving the intended regulatory outcome.

The action: What operators are already doing

The mobile industry continues to invest heavily in robust security measures to protect its customers, assets and services. Operators embed resilience in network planning and operations, drawing on extensive experience of managing physical and operational risks to service availability, performance, and functionality. Measures include hardening sites, providing reliable backup power and deploying rapid-response assets such as mobile cells and portable generators. Where feasible, operators also build network redundancy through diverse fibre routes, automatic failover, overlapping radio coverage, satellite backhaul and emergency roaming agreements. Together, these measures help maintain or restore connectivity during localised failures, disasters, and wider outages. Operators also invest in training and equipping staff with the skills and tools needed to respond effectively.

A recent GSMA Intelligence study on Europe's mobile investment needs projects that operators worldwide will invest $1.5 trillion in infrastructure between 2023 and 2030[1], while making Europe's critical mobile infrastructure resilient will require €38 billion.[2] A GSMA report on climate risk and resilience estimates that severe storms and floods currently cost mobile operators $1.7 billion a year in cell-site repairs and replacement worldwide. Under projected mid-century climate conditions, this could rise by around 80% to $3.1 billion a year. These costs are equivalent to about one percent of estimated current global mobile operator capital expenditure.[3]

Policy principles for developing mobile network resilience

The GSMA has developed the following policy principles to guide governments and regulators in designing resilience frameworks that help enable operators to make investment decisions that support innovation in infrastructure and technologies, strengthen mobile network resilience, and enhance public trust in digital services. For operators, this means governments and regulators should design and implement frameworks that are proportionate, risk- and outcome-based, and encourage collaboration and dialogue across the wider ecosystem.

1 www.gsma.com/about-us/regions/europe/wp-content/uploads/2026/05/Mobile-Investment-Needs-in-Europe-GSMA.pdf (May 2026)
2 Accounts for the cost of extending base-station battery life, satellite backhaul, engine-powered/solar generators and further increasing cybersecurity
3 Futureproofing Connectivity - Climate Risk and Resilience in Telecommunications.

Principle A: Avoid prescriptive regulation and promote outcome-based policy that supports sustained investment.

Ensure obligations focus on risk-based, practical outcomes rather than prescriptive inputs, and sustain long-term investment that resilience depends on.

Resilience requires sustained investment in infrastructure, power, security, monitoring, people, and operational capability. This involves additional costs, often met by redirecting investment from network coverage, capacity, technology, and performance, or through higher consumer prices. Governments and regulators should recognise these trade-offs when assessing whether proposed measures are proportionate to the expected resilience benefit. Operators need sufficient flexibility and funding to choose the most effective combination of prevention, redundancy, response, and recovery measures for the risks they face, supported by clear and predictable obligations that enable long-term planning and investment. Regulatory policies and frameworks should therefore be technology-neutral, economically realistic, proportionate, risk-based, and targeted where they deliver the greatest benefits to consumers and society. Their effectiveness should be judged by the resilience they achieve, not simply by compliance. Governments should avoid rigid technical rules that apply uniformly across different geographies, sites, and risk profiles. For example, sites serving emergency services, hospitals, transport hubs, government facilities, or other critical infrastructure may warrant stronger measures than lower-risk locations. Sites that are difficult to access during a disaster may also require greater protection against mains power loss. Where resilience requirements exceed operators' risk-based investment plans, governments should consider appropriate incentives, funding, or cost-recovery arrangements.

Principle B: Build upon resilience-by-design.

Support operators with the flexibility to use the most appropriate mix of technologies and solutions and adapt as innovation evolves.

Network investment decisions have long-term consequences and need outcome-based government policies that are not overly prescriptive, to help strengthen resilience to both current and future risks. These include climate-driven extreme weather, power outages, theft, damage, and geopolitical events. Operators already embed security and adaptability from the outset which reduce risk and maintain connectivity and service continuity during incidents.

Governments can play their part by supporting technologies such as AI-enabled automation that strengthen connectivity during crises, as well as equipment, backup systems and climate-resilient site planning. In close consultation with mobile operators, governments should use flexible infrastructure policy, planning rules, permitting, emergency preparedness and regulatory frameworks to promote resilience outcomes rather than compliance alone.

Principle C: Consult early and design with operational reality.

Strengthen dialogue and inclusive consultation between governments, regulators, mobile operators, and other relevant sectors.

Regulation is most effective when informed by the organisations that build, operate and restore networks. When considering new obligations, governments and regulators should engage meaningfully with operators and the wider resilience ecosystem to account for dependencies on other critical infrastructure, particularly energy supply, physical security, and site access. Proposals should be supported by evidence-based impact assessments and ongoing review to ensure measures remain proportionate, practical and effective. They should also consider feasibility, cost, implementation timelines and constraints such as restricted access, theft and vandalism. When developing policies or frameworks, regulators should review existing rules and remove overlapping, conflicting or misaligned requirements. Frameworks should provide long-term certainty while remaining flexible enough to accommodate emerging technologies, evolving operational practices and a changing threat landscape. Industry- or operator-led frameworks can offer significant advantages: they can be developed, implemented, and adapted more quickly as circumstances change, while securing greater industry support than highly prescriptive, top-down requirements.

Principle D: Develop resilience policy as a cross-sector responsibility.

Ensure coordination between governments, emergency services, the telecoms industry, energy providers, and other relevant sectors before and during incidents.

Network resilience increasingly depends on interconnected sectors, including energy, transport, cloud services, and wider digital infrastructure. Mobile networks form part of this ecosystem and rely on power, fuel, physical security, and access to damaged or restricted sites. Policies and frameworks should recognise these interdependencies and enable coordinated planning before, during and after major incidents. Governments should establish clear, structured engagement mechanisms involving telecoms, energy, transport, emergency services, public safety agencies, and local, regional, and central authorities. These mechanisms should promote shared accountability and cross-sector planning for early warning systems, crisis management protocols, emergency communications, intelligence sharing (subject to confidentiality safeguards) and priority access to critical sites. All organisations should develop and test plans, conduct joint exercises, share lessons from incidents, and identify barriers to implementing resilience measures effectively.

Principle E: Enhance trust through clarity, transparency, and continuity.

Promote public confidence through clear responsibilities, effective communications, and continuity of essential services.

Public confidence depends on clear responsibilities, credible preparedness, and timely communication during disruptions. Resilience frameworks should support education and awareness, clear accountability, trusted intelligence-sharing and sustained public-private collaboration, both nationally and across borders where shared systems and supply chains can spread disruption between neighbouring markets. They should also provide clear, enforceable government and regulatory support that enables operators to maintain critical communications during national emergencies and geopolitical events. This includes emergency calls, public warnings, practical and actionable customer information, support for vulnerable users and priority services. Transparency and intelligence-sharing requirements should be proportionate and safeguard commercially sensitive and security-related information, sustaining trust and operational focus without creating unintended security risks.

The outcome: putting the policy principles into practice

Governments and regulators should put these policy principles into practice through structured dialogue, evidence-based assessment and coordinated implementation plans tailored to local market and regulatory conditions. This should include reviewing whether existing frameworks strengthen resilience or merely add cost and complexity. Effective frameworks are risk-based, outcome-focused, supportive of investment and coordinated across relevant sectors. They should give operators the flexibility to deploy appropriate solutions while assuring governments that preparedness, restoration, and public communications are robust.

The GSMA and its members stand ready to support this work by sharing operational evidence, lessons from incidents, international examples, and practical expertise. The goal is clear: regulation that keeps society connected when it matters most.



GSMA Head Office
One Angel Lane
London, U.K.
EC4R 3AB
United Kingdom
gsma.com

