DELL Technologies

Dell's Corporate Security and Resilience

An Overview

Dell Technologies Security & Resilience • Version 1.10 • Last Updated 10-10-2023

At Dell Technologies, we think deeply about how we build trust and secure a connected world. With the emergence of a connected, intelligent world, 5G and advanced technologies like AI and machine learning, we can do more than we ever imagined. We will be secure, resilient, and adaptive to our ever-changing world. And we will continue to live our overarching mission – to protect Dell Technologies and earn our customers' trust by embedding security and resilience into everything Dell does.

John Scimone, Chief Security Officer

Security & Resilience Organization

Protect Dell Technologies and earn our customers' trust
by embedding security and resilience in everything Dell does.

Cybersecurity

Protecting customer and company data

Advanced threat intelligence with visibility of emerging threats

Identity and access management

Managing cyber risk, maintaining compliance, and appropriately securing our environment

Enterprise Resilience, Global Investigations & Corporate Security

Enterprise Resilience Security

Corporate Security: managing the protection of people, information, assets and our reputation from physical and environmental attacks and events.

Crisis Management: managing unexpected events that may negatively impact Dell Technologies.

Business Continuity: ensuring timely recoverability of business-critical processes and operations.

Disaster Recovery Governance: ensuring timely recoverability of business-critical data and systems.

Global Investigations: managing physical incidents such as theft, fraud, and workplace violence.

Product & Application Security

Vulnerability Response: promptly respond to reported vulnerabilities to keep deployed products and applications secure.

Secure Development Lifecycle: develop more secure products and applications by building security into the development lifecycle.

Governance, Risk & Compliance

Creating, maintaining, and ensuring compliance of Dell Technologies Security & Resilience Policies, standards, and processes

Ensuring compliance with external regulations like Sarbanes-Oxley act (SOX) and Payment Card Industry Data Security Standard (PCI DSS)

Performing audits, renewing contracts (where Dell is a vendor to the customer) and providing customers with information about security rules and protocol for Dell's products and services.

Dell Federal | Dell Technologies Services | Dell Financial Services

Cybersecurity

Cybersecurity sets standards for, and implements and maintains, security programs and technology that helps Dell Technologies manage and mitigate risk, and helps protect our information, our business, our customers, and our brand against advanced adversaries.

Cybersecurity at Dell Technologies is responsible for:

- Protecting customer and company data
- Advanced threat intelligence with visibility of emerging threats
- Identity and access management
- Managing cyber risk, maintaining compliance, and appropriately securing our environment

Why focus on Cybersecurity?

4.5 hours

Average breakout time for threat actors to move within a company's network after initial compromise

$6 trillion

Projected cost of breaches worldwide by 2021

78 days

Average time it takes to detect a sophisticated intrusion

Product & Application Security

Product and Application Security involves ensuring products offered to customers are protected against cyber threats and free of vulnerabilities.

Product and Application Security at Dell Technologies is responsible for:

- Secure Development Lifecycle — develop more secure products and corporate applications by building security into the development lifecycle
- Vulnerability Response — promptly respond to reported vulnerabilities to keep deployed products and applications secure

Why focus on Product & Application Security?

90%

of security incidents result from exploits against defects in products

100x

increase in cost to fix software defects in maintenance phase vs cost of fixes in design phase

~60%

of breaches typically involve a vulnerability for which a patch was already available

Global Security Operations

Global Security Operations involves the protection of people, information, assets and our reputation from physical and environmental attacks and events. Global Security Operations at Dell Technologies is responsible for:

- Protecting our people, processes, assets, and the Dell Technologies brand across the globe
- Managing guards, security cameras, investigating crimes and non-cyber security incidents committed against the company by employees and criminals

Examples of Global Security Operations examples and actions:

- Crisis Management
- Business Continuity
- Disaster Recovery
- Insider Risk Management
- Investigation of crimes and code of conduct violations
- Uniformed Security Guard Services
- Facility Security Systems
- Event Security
- Enhanced Protection for High-Risk Personnel
- Secure Transportation of Key Personnel and Assets
- Manages intake of all security-related matters via Security@Dell.com

Why focus on Global Security Operations?

$9k

the cost of an unplanned data center outage per minute

21%

of annual security breaches attributable to physical and insider theft

2M+

violent workplace incidents in the U.S. annually

78%

of workplace homicides are shooting deaths

Organizational Security

At Dell we ensure that our global team members are aware that it is their responsibility to comply with security and resilience practices and standards. To facilitate the corporate adherence to our practices and standards, the function of our information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.
2. Security testing, design, and implementation of security solutions to enable security controls adoption across the environment.
3. Security operations of implemented security solutions, the environment, and assets, and manage incident response.
4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

Your trust, our transparency

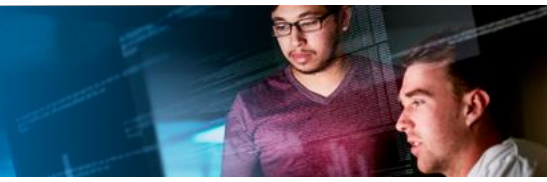
Dell's digital transformation journey is based on the same pillars that we use to empower our customers: Business Transformation, IT Transformation, Workforce Transformation, and Security Transformation. We adopt and follow the "intrinsic security" principle in all the systems and solutions that support our business processes; and customize the use of proven frameworks and methodologies that ensure alignment with our corporate strategy. In addition to ensuring that we prioritize security controls, like those recommended by the Center for Internet Security (CIS) and the SANS Institute, we also keep track of what our customers care about the most. Below are the top 20 controls about which our customers request information most often. We have grouped these controls based on the five highest-level functions as defined in the NIST Cyber Security Framework (CSF).





Identify	Protect	Detect	Respond	Recover
Asset Management	Access Management	Anti-Malware	Business Continuity	Disaster Recovery
Compliance	Data Governance	Change Management	Incident Management	
Risk Management	Dell Employment	Logging and Alerting		
Supply Chain	Encryption	Vulnerability Management		
	Network Management			
	Password Management			
	Patch Management			
	Physical Security			
	Secure Development Lifecycle			

Identify

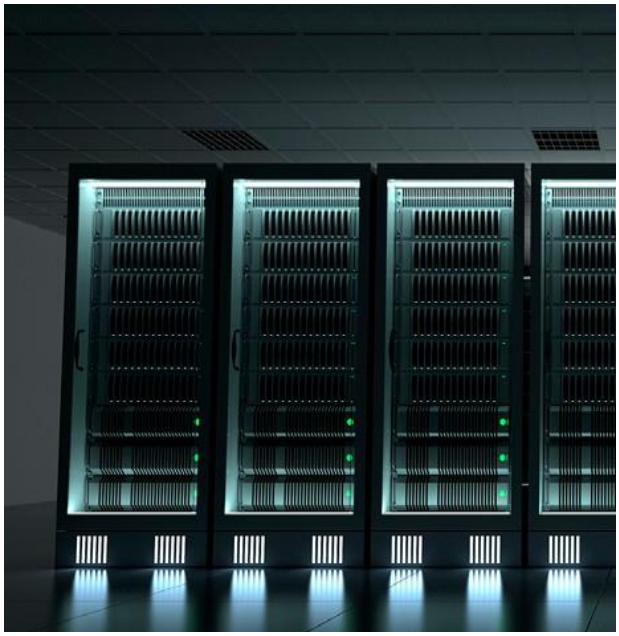


Asset Management

Dell's practice is to track and manage physical and logical assets. Examples of the assets that Dell IT might track include:

- Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information.
- Software Assets, such as identified applications and system software.
- Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers, and communications equipment.

Identifying, tracking, and managing information, software, and physical assets are very important at Dell. Dell has a robust Asset Management Program with rules and activities communicated to all personnel. All assets are accounted for, have a nominated owner, and are provisioned and monitored until depreciated and returned.



The assets are classified based on business criticality to determine confidentiality, integrity, and availability requirements. Industry guidance for handling personal data provides the framework for technical, organizational, and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

The Use of Company Resources Policy applies for all company-owned information technology resources, regardless of location and outlines multiple requirements to ensure Dell employees clearly understand what is considered acceptable use of such assets.

Compliance

Our Security & Resilience Organization's portfolio of policies, standards, polices and controls align to NIST and ISO frameworks. Those foundational rules cover the full lifecycle of data, our physical and cyber environments as well as each team member's responsibility to contribute to our security culture. Information Security, Legal, Privacy and Compliance departments work to identify all applicable regional laws and regulations. These requirements cover areas such as intellectual property of the company and our customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

We have multiple mechanisms in place to ensure compliance with such requirements which include: the information security program, the executive privacy council, executive risk steering committee, global risk and compliance council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessments, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management. Additionally, a variety of independently audited and certified security accreditations are in place, based on the geographical and business need, including SOX, ISO27001, SOC1, SOC2 and PCI DSS.

Our Code of Conduct provides guidance on how we carry out our daily activities across Dell Technologies in accordance with our culture and values, as well as in compliance with the letter and spirit of all applicable laws in the countries in which we work and serve.

Risk Management

We have an established risk management program to provide adequate processes for identifying, evaluating, and treating risks around the organization's valuable information. It addresses uncertainties around those assets to ensure the desired business outcomes are achieved.

Our risk management program utilizes an integrated control and risk framework that focuses on the key business needs of availability, access, accuracy, and agility pertaining to information technology and information security. It provides the structure and discipline to ensure that our information technology and information security risk is continuously evaluated and addressed in a proactive, cost effective manner, including people, processes, data, and technology. Risks are documented and managed through the management action plan/remediation process (MAP), each having a risk owner assigned and accountable for remediation.

Supply Chain

We take a holistic and comprehensive approach to protect its supply chain and deliver solutions that customers can trust. Our strategy of defense-in-depth and defense-in-breadth involves multiple layers of controls to mitigate risks that could be introduced in the supply chain. These controls help establish supply chain assurance, defined as the confidence that the aggregated set of processes and controls throughout the supply chain and product lifecycle will produce and deliver products, processes and information that are free of unintended elements and that function as designed and intended.

Our supply chain risk management framework mirrors a comprehensive risk management framework of the National Infrastructure Protection Plan (NIPP), which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Our framework incorporates an open feedback loop that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle.

Supplier governance is critical to safeguarding the performance and integrity of the supply chain and because of it, our supplier governance begins with a thorough review of potential suppliers and partners prior to onboarding. Analysis prior to awarding work may include initial site surveys and manufacturing qualification builds in conjunction with the completion of the product-specific request for information (RFI) or quote (RFQ). We are uniquely positioned to leverage insights, best practices, technology, and expertise from industry-leading, trusted and respected brands in the Dell Technologies portfolio like Pivotal, RSA, SecureWorks, Virtustream, and VMware. We believe that it is critical to listen to and work with customers, suppliers, and partners to continue to improve how Dell delivers supply chain assurance.

Protect

Access Management

Managing the lifecycle of digital identities and their access to Dell resources is a crucial factor in protecting Dell's network and systems. The digital transformation has quickly moved out of the traditional data center and into the cloud, creating significant risk in the form of ransomware and loss of data. Our Identity and Access Management policies help ensure an increased security posture, regulatory compliance, and operational excellence through automation and risk-based prioritization.

Tight identity management, "least privilege" user access, and multi-factor authentication helps meet the risk associated with hybrid, multi-cloud, and edge environments. Dell's approach includes proper governance for employee and contractor on-boarding, transfer, and termination. Robust real-time analytics and reporting further enable operations and assurance teams to deliver a contemporary user experience while ensuring that digital identities (people, devices, and applications) have the "right access to the right resources at the right time."

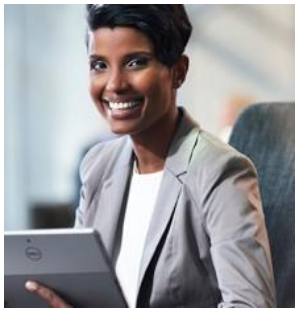
Data Governance

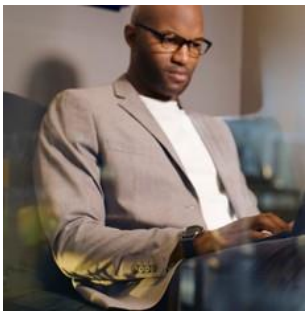
Our mature enterprise information governance framework includes requirements for the lifecycle of hard copy and electronic data and information. It covers the creation, receipt, management, processing, storage, and disposal of all information used in the normal course of business, regardless of format or media. The information security and privacy guidelines cover the identification, classification protection, retention and disposal of all application/databases and documents in approved repositories/storage locations.

- Information assets are identified and inventoried according to their location and movement throughout their lifecycle.
- Structured and unstructured data is classified according to the adopted Data Classification Categories (Public, Internal Use, Restricted and Highly Restricted). When information falls into more than one classification, the most restrictive classification label is applied. Assets are classified based on business criticality to determine confidentiality requirements.
- Based on the data's value, use and purpose, protection requirements are set for each data classification category from the point of its creation, through the end of its lifecycle. Industry guidance for handling personal data provides the framework for technical, organizational, and physical safeguards.
- Information is retained per its retention period requirement based on legal or regulatory requirements, including legal hold, and operational business needs.
- Secure disposal of information occurs once the retention period requirement period has expired.

Dell Employment

The controls that we have in place cover background verification and competence checks on all candidates for employment, to ensure that our employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. These checks are carried out in accordance with the relevant laws, regulations and ethics and are proportional to the business requirements, the classification of the information that will be accessed and the perceived risks associated.

As part of the employment process, all our employees and subcontractors must sign a non-disclosure agreement and undergo a screening process applicable per regional law.

Encryption

Our policies for cryptography in accordance with industry best practices. Also, the standards and controls that support our policies are dynamically aligned to the business and legal requirements that our stakeholders demand.

We establish and manage cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction. Cryptography is implemented for data with a specific classification as outlined in the relevant policies or standards adopted. Our wireless network is secure using the best industry standard cryptographic methods.

Our cryptographic processes and systems provide services for data at rest, in use, and in motion which includes support for infrastructure, databases, and applications. Additionally, our strong cryptographic key management process ensures that keys, certificates, and digital signatures, are secured along their lifecycle. This includes generation, distribution, storage, backup, rotation, expiration, archival, and destruction.

Network Management

Dell implements necessary network safeguards such as employing technical and administrative controls to manage the security of the network and supporting infrastructure.

Our controls are aligned to NIST and the Center for Internet Security for securing and hardening network devices. Network management provides connectivity to the internet, local network, and remote access to our resources, along with network design standards that provide the foundation from which we secure the network services it provides to users. Through administrative, physical, and technological controls, which are implemented in accordance with industry best practices, we ensure a secure environment based on layers of protective components that support and complement each other, to increase the overall security.

Password Management

Dell recognizes that it is imperative for our users to practice due diligence for gaining access to our systems by protecting their user accounts with passwords which are not easily guessed or deduced. Passwords are an important aspect of computer security and are the first line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network, so all employees, contractors, and third parties with access to systems, are responsible for taking the appropriate steps in selecting and securing their passwords as well as adhering to 2-factor authentication to access our internal network.

Password policy and standards, in line with industry standards, are in place to ensure that secure practices are maintained by all users, and they support protected information infrastructure strategy. These include, among others, the creation of strong passwords, protection of those passwords, and the frequency of change. Additionally, we make use of logging, monitoring, automation, and alerting systems that enforce password policies and provide an additional security layer.

Patch Management

We maintain a global patch management program which follows industry standards and meets regulatory and compliance requirements. Our patch management process is in accordance with security best practices and includes:

- Maintaining current knowledge of available patches
- Inventory list of all our assets that will require patching with the use of automated monitoring tools
- Determining which patches are appropriate for particular systems, ensuring proper testing
- Installation under change control management program
- Reviewing patch process and results and documenting all associated procedures, such as specific configurations required, standard and emergency patching procedures

Our applications and new and existing systems are maintained to the latest security patching levels.

Physical Security

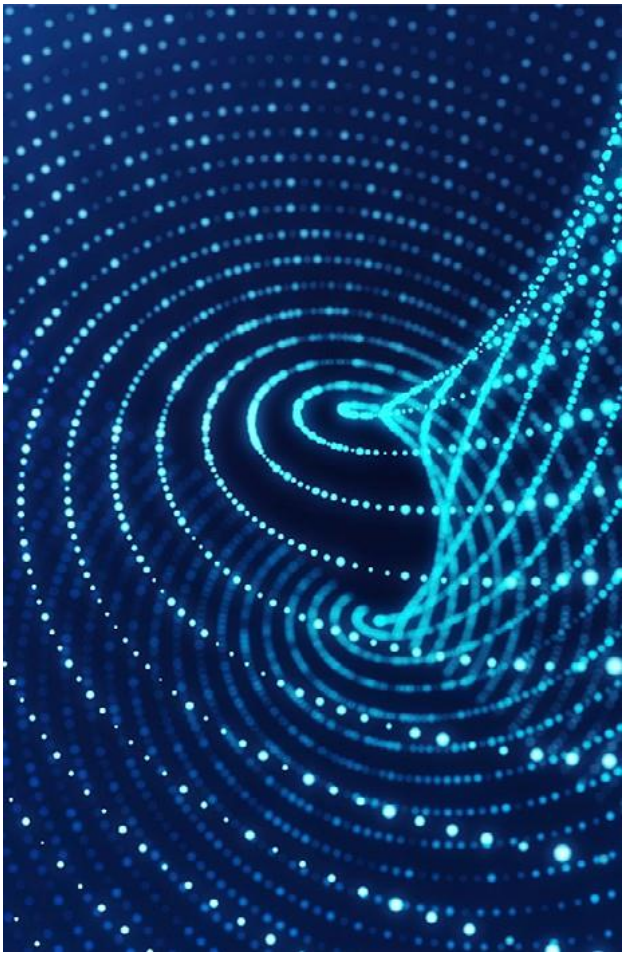
Computing facilities are one of our most valuable assets and must be protected. Physical access restriction to authorized personnel, as well as robust environmental controls, protects the confidentiality, integrity, and availability of our data and computing environments from a wide range of threats to ensure business continuity, minimize business impacts, and maximize return on investment and business opportunities.

The physical security program follows industry security best practices and regulatory requirements to ensure that physical access to our facilities that conduct business are controlled with secure physical entry points to prevent unauthorized access, damage, and interference to premises and information. Access to facilities that contain critical or sensitive information is controlled to restrict personnel with valid authorized business need and reviewed regularly to ensure only appropriate personnel have access.

Secure Development Lifecycle

We utilize a robust system development lifecycle to control the steps that must be taken to ensure that all hardware, software, and firmware that is distributed to customers (internal and external) have been appropriately designed, developed, and packaged under the structure of a formal governance program and as defined by the development lifecycle.

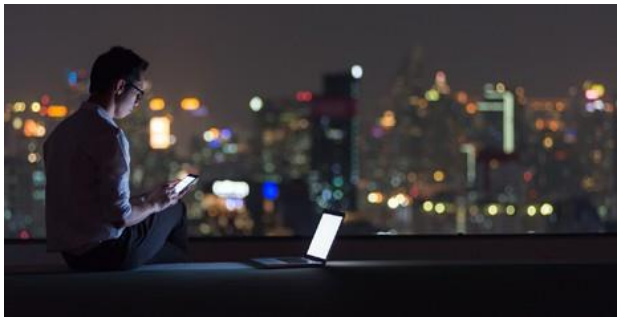
We endeavor to embed security throughout the product or application lifecycle, so every product and application is built securely and remains secure. Dell's security program includes analysis activities such as threat modeling, static code analysis and security testing to discover and address security defects throughout the development lifecycle.



Dell's Secure Development Lifecycle program is aligned with the principles outlined in ISO/IEC 27034 'Information technology, Security techniques, Application security.' Dell also collaborates through many industry standard venues such as SAFECode, BSIMM, and IEEE Center for Secure Design to ensure we follow industry practices.

Additionally, many Dell employees are actively involved in organizations which focus on developing security standards and on defining industry-wide, security practices, including:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- The Forum for Incident Response (FIRST)
- International Committee for Information Technology Standards (INCITS)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)



Publicly released third party vulnerabilities are regularly reviewed to determine their impact and applicability in our environment. Based on the risk they pose to business and customers, there are pre-determined timeframes for remediation. In addition, by using a proactive and risk-based approach, we perform periodic vulnerability scanning and assessments of our applications and infrastructure. Moreover, secure code reviews and vulnerability scanners are used along the development process and prior to be released to production; to proactively detect coding vulnerabilities or risks.

Detect

Anti-Malware

We have implemented multiple controls for the detection, prevention, and recovery, combined with an appropriate awareness program, to protect its environment against any malicious software and viruses.

We utilize a multi-level centrally managed antivirus and endpoint detection and response (EDR) protection model, including three levels of gateway protection from three industry leading vendors. We have a defined and standard set of solutions which is installed on all devices in scope. Those devices must remain operational and adherent to configuration settings supplied by the managing policy server and process, as appropriate for the operating system. Additionally, our anti-malware program requires that all inbound and outbound messages are scanned for spam, virus, DLP policies, attachment protection, phishing, and bulk emails.

Change Management

We have implemented an industry best practice change management process to ensure that its production line assets are stable, controlled, and protected.

Our change management process ensures that changes to IT resources are managed in a controlled manner, so that they cause minimum disruption to the business. Change management provides the requirements, guidance and tools needed to govern these changes, to ensure that they undergo the appropriate reviews, approvals, and that are communicated effectively to users.

Below is a list of some of the benefits:

- Minimize operational risk of necessary changes
- Maximize effectiveness of implemented changes
- Facilitate centralized prioritization and scheduling of all changes within the environment
- Simplify future changes through clear documentation and well-defined processes
- Deliver consistent, predictable service levels for all types of changes to the environment
- Increase ability to process high volumes of changes
- Prevent change conflicts through a central scheduler

Logging and Alerting

We have established and maintain a logging and alerting management program which follows industry standards, regulatory, and compliance requirements for logging events and tracking authorized and unauthorized activity and access to systems, applications, and data.

Our logging and alerting program ensures capturing, notification, tracking, and management of security events for systems, applications, platforms, and network devices as deemed by their business classification and criticality. As part of the program, we have implemented controls for standardizing logs, their retention, and to protect those from unauthorized alteration. Additionally, the normalized format of the details captured in the logs, facilitates event management and their identification by type, location, subject, user, datetime stamp, and even what data was accessed.

Last of all, we use real-time monitoring methods to monitor, generate alerts on suspicious activity or when an audit log failure occurs, and even trigger automated remediation for well-known events.

Vulnerability Management

To meet the enterprise business objectives and ensure effective protection of our environment and operations, we have established a global security patching and vulnerability management strategy. Numerous controls are in place to ensure that our environment is carefully managed to maintain effective protection against internal and external threats. We protect the integrity, availability and confidentiality of data, applications, infrastructure, customer data which aligns with industry standards.

As part of our vulnerability management strategy, cyber threat information is compiled from trusted resources and alliances are formed with key vendors. Our assets and systems are scanned for vulnerabilities. Patching and remediation are executed based on our policies, priorities, and potential risk impact.

Respond

Business Continuity

Dell's fast-paced, global business requires a flexible approach to operational resilience, so we can respond to risks with minimal downtime and provide an adaptable infrastructure to enable growth while protecting the interests of our customers, employees, business partners, and stakeholders. We have integrated a global business continuity program that defines the framework of our operational resilience standards and assists Dell business units in planning for and mitigating risk, to ensure we are meeting our customers' needs in an ever-changing world.

The enterprise resilience program is risk-based by design and aligned to recognized international industry standards including ISO 22301. It directs business units to specify alternate and recovery procedures for the loss of key functional dependencies. They do so in a manner which enables the company to maintain service provision without impacting service levels, Recovery Point Objectives (RPO), and/or Recovery Time Objectives (RTO) as per agreement with customers. A Business Impact Analysis (BIA) is used to define the most critical functions.

Security Practices

Overall guidance for Dell's program is provided by the Global Business Continuity Office (GBCO) and is led by staff with subject matter expertise and certifications in business continuity practices. The GBCO provides guidance to the company on how to avoid, prepare and recover from a business interruption, with a best-in-class Business Continuity program on par with a tier one supplier. The program directs business units to specify alternate and recovery procedures for the loss of key functional dependencies, in a manner which enables the company to maintain service provision without impacting service levels, Recovery Point Objectives (RPO), and/or Recovery Time Objectives (RTO) as per agreement with customers. A Business Impact Analysis is used to define the most critical functions.

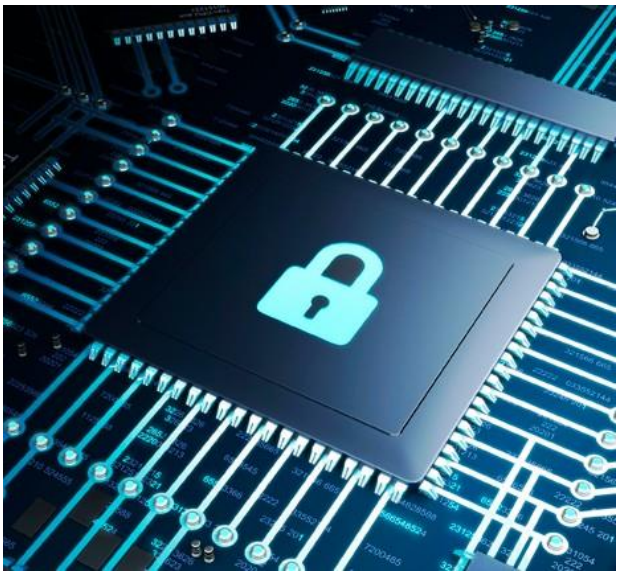
Dell’s business continuity planning process includes a corporate policy which demonstrates a commitment to a global, business-wide approach and is supported by senior management. The Business Continuity Plans address critical scenario planning to include continuity and recovery from the loss of:

- Human capital and subject matter expertise
- Critical infrastructure
- Facilities
- Assets including vital documents, IP, critical data
- IT applications and infrastructure
- Critical internal and external dependencies
- Vendor managed and 3rd party services

Dell requires all critical business functions to refresh and test their Business Continuity Plans annually.

Communication

A Communication Plan has been established which ensures that key decision-makers and subject matter experts are able to collaborate during the threat of a business interruption. The Communication Plan includes contacting customers when the company is under threat of a business interruption which could impact them.



Risk Assessment

A risk assessment is performed annually to determine and prepare for the natural and man-made events most likely to impact business operations.

Vendors/Third Parties

Dell policy requires the enforcement of business resilience standards upon vendors by assessing vendor capability, monitoring compliance at regular intervals, establishing alternate sourcing, and having a plan to handle counterfeit, stolen or illegal items.

Regulatory Compliance and Related Programs

Dell has established procedures and policies necessary to maintain compliance with applicable product and operational laws and regulations, such as workplace safety, product safety, environmental protection, labor standards, building codes, and import/export compliance. In addition, key locations and/or business processes are certified to relevant voluntary standards including ISO 9001, ISO 14001, OHSAS 18001, ISO 20000, and others. Dell’s procedures and processes are adjusted as needed to reflect changes in internal operations and external factors (e.g., climate change, population growth, and access to energy and water).

Security

Physical security controls and procedures have been established to monitor, deter, detect, and protect critical assets which support Dell service provision from physical threats. Such procedures are commensurate to the assessed risks and asset value and are routinely checked for effectiveness. Relevant data security controls, including access control, encryption, and information classification have been established to protect both Dell and customer data. There is also a plan to ensure the safety and security of our employees and to mitigate the impact of possible work stoppages due to unforeseen workforce reductions.

Sustaining & Continuous Improvement

Dell requires management to review and approve the continuity and recovery strategies at least annually. Dell businesses are required by company policy to analyze operational processes for risks and single points of failure and to implement strategies to close any unacceptable gaps.

If you have further questions regarding Dell’s Business Continuity Program, please contact your Dell account representative.

Incident Management

The primary objective of the cybersecurity incident response program is to mitigate and contain the risk associated with computer security incidents.

Protecting our reputation and relationships is of utmost importance to the company. An effective end-to-end cybersecurity program plays a key role in establishing this protection by helping safeguard the company’s information and assets. Our cybersecurity incident response plan is a critical component of such a program and is intended to outline how we identify, assess, respond to, and remediate cybersecurity incidents. The plan also defines roles and responsibilities among various stakeholders who participate in our response to a cybersecurity incident.

A corporate response plan for cybersecurity incidents is in place and outlines purpose, scope, identification, assessment, response, and remediation of security incidents, including notifications to regulators, controllers and/or data subjects as may be required.

Recover

Disaster Recovery

We recognize the importance of having a consistent, scalable, flexible, and coordinated approach to resilience in the increasingly uncertain and challenging global environment in which we operate.

If an incident severely impacts our ability to conduct business as usual, our disaster recovery program provides for timely restoration of business-critical processes, applications, data, and systems that support our critical operations.

The disaster recovery program establishes standards, processes, and controls for the timely recoverability of business-critical data, application, systems, and infrastructure used to manage and support our business functions. These requirements ensure the continuity of resources that support our critical business functions.

Our program and methodology ensure that applications and infrastructure, that serve our customers, possess resilience capabilities that are aligned with contractually obligated service level agreements, RTO, and RPO. A designated recovery site, as well as availability of IT disaster recovery personnel, have been pre-established to be quickly mobilized in the event of a business interruption. Additionally, the disaster recovery plans are revised and tested at least annually, when new applications are brought online, or when changes to the IT environment occur. The test methods are commensurate to the criticality of the application/system.