AI IMPACT REPORT NO. 216 · REVISED 5 OCTOBER 2026 · 250 ROLES COVERED

Network and Computer Systems Administrators

AI profoundly augmenting monitoring, troubleshooting, and automation of IT infrastructure.

EXPOSURE	WINDOW	ADOPTION TODAY	READING
63 High exposure	2–5 yrs until change lands	High	Substantial automation of routine work. Exposure is the share of today's work AI can plausibly take on within the window.

§ 01 WHAT IS HAPPENING

What is happening to network and computer systems administrators

Impact

AI tools are automating routine monitoring, identifying sophisticated anomalies, streamlining diagnostics, and enhancing proactive remediation. This shifts Network and Computer Systems Administrators' focus towards strategic infrastructure planning, complex problem-solving, ethical oversight of AI systems, and proactive risk mitigation.

Risk

Significant augmentation; emphasis on strategic infrastructure, advanced troubleshooting, and AI tool mastery.

The Network and Computer Systems Administrator role will be heavily augmented by AI. AI will handle much of the high-volume log analysis, alert correlation, and initial troubleshooting. Administrators will need to become experts in leveraging AI tools, critically evaluating AI-generated insights, understanding the limitations and biases of AI in IT operations, and focusing on complex incident investigation, proactive optimization strategies, and human-centric systems architecture. Ethical considerations of AI in automation and data privacy will be paramount.

Sector readiness

Rapid & Deep Integration

The IT operations and infrastructure management sectors are making substantial investments in AI for monitoring (AIOps), automation, and security. Given the high-stakes nature of system reliability, performance, and security, integration is rapid and deep, with emphasis on validation, explainability, and compliance in critical IT systems.

§ 02 POSITION

Where you stand

i The Network and Computer Systems Administrator role is undergoing a profound transformation, with AI becoming a critical partner in every aspect of IT infrastructure management.

ii AI will automate routine monitoring, initial troubleshooting, and repetitive tasks, allowing administrators to focus on high-level strategic planning, complex incident resolution, and ensuring the resilience and security of advanced IT systems.

iii Success will increasingly depend on mastering AI tools, critically validating their outputs, and developing deep interdisciplinary skills to navigate the complexities of AI-enabled IT operations and cloud environments.

§ 03 ACTIONS 15 POINTS

What this means for you

Concrete changes to how the work gets done, in the order you are likely to meet them.

01 **AI-Enhanced System Monitoring & Anomaly Detection (AIOps).** Network and Computer Systems Administrators are leveraging AI systems to process vast amounts of operational data (logs, metrics, traces) from servers, networks, and applications. AI autonomously correlates alerts and identifies subtle anomalies that indicate impending issues or security threats, significantly reducing alert fatigue and speeding up problem identification.

02 **Predictive Maintenance & Proactive Issue Resolution.** Network and Computer Systems Administrators will utilize AI models that analyze historical performance data and current trends to predict infrastructure failures (e.g., server crashes, network outages) before they impact users. This enables proactive maintenance and intervention, minimizing downtime and service disruptions.

03 **Intelligent Root Cause Analysis (RCA).** When an IT incident occurs, AI tools are assisting Network and Computer Systems Administrators in rapidly pinpointing the root cause by analyzing vast amounts of log data, system configurations, and error traces. This accelerates debugging and ensures faster resolution of identified issues, reducing Mean Time To Resolution (MTTR).

04 **Automated IT Operations (IT Automation).** Network and Computer Systems Administrators will increasingly oversee AI-powered automation platforms that autonomously execute routine IT tasks, such as patch management, backup verification, user account provisioning, and basic system configurations, freeing up significant manual effort.

05 **AI-Driven Network Optimization.** Network and Computer Systems Administrators are employing AI for dynamic network optimization. AI analyzes traffic patterns, bandwidth utilization, and device performance to suggest optimal routing paths, reconfigure network devices, and prevent congestion, ensuring high network availability and speed.

06 **Cloud Resource Optimization & Cost Management.** With pervasive cloud adoption, Network and Computer Systems Administrators are using AI-powered tools to continuously monitor cloud environments for misconfigurations, underutilized resources, and cost inefficiencies. AI provides automated remediation suggestions and optimizes cloud spend.

07 **AI in Security Operations (SecOps).** Network and Computer Systems Administrators are integrating AI into security tools (e.g., SIEM, EDR) to enhance threat detection, identify anomalous user behavior, and automate responses to security incidents. This strengthens the overall security posture by proactively identifying and mitigating threats.

08 **Generative AI for IT Documentation & Scripting.** AI is streamlining the creation of technical documentation. Network and Computer Systems Administrators will use AI to automatically generate initial drafts of system configurations, network diagrams, troubleshooting guides, and automation scripts, ensuring consistency and accuracy.

09 **Human-AI Teaming in Operations Centers.** Network and Computer Systems Administrators will increasingly operate in human-AI teams within Network Operations Centers (NOCs) or Security Operations Centers (SOCs). AI acts as an intelligent co-pilot, providing real-time alerts, suggesting investigation paths, and automating initial responses, allowing human administrators to focus on complex, strategic issues.

10 **Ethical AI & Data Privacy in IT.** Network and Computer Systems Administrators will need to critically assess the ethical implications of AI tools in IT (e.g., monitoring employee behavior, automated access control). This involves understanding potential biases in AI outputs, ensuring data privacy, and upholding organizational policies.

11 **AI-Assisted Capacity Planning.** Network and Computer Systems Administrators are leveraging AI to analyze historical usage trends and predict future demands for computing, storage, and network resources. This enables more accurate capacity planning and prevents resource bottlenecks.

12 **Automated Incident Response & Remediation.** AI is powering automated incident response playbooks that can autonomously isolate affected systems, block malicious IPs, and initiate basic recovery steps following a security breach or system failure, reducing response times.

13 **Continuous Learning & Specialization.** The dynamic nature of IT infrastructure, cybersecurity threats, and AI advancements requires Network and Computer Systems Administrators to continuously learn about new AI systems, automation tools, and specialized technical areas (e.g., cloud ops, SecOps).

14 **AI-Driven Performance Optimization for Applications.** Network and Computer Systems Administrators are collaborating with AI tools that analyze application performance in real-time, identifying bottlenecks in infrastructure (network, server, storage) that impact user experience. AI suggests optimizations to improve application responsiveness.

15 **Strategic Infrastructure Planning & Architecture.** As AI automates routine tasks, Network and Computer Systems Administrators will dedicate more time to high-level strategic infrastructure planning, designing resilient and scalable systems, and aligning IT architecture with overall business objectives.

§ 04 CAUSES 10 DRIVERS

What is pushing this change

01 **Increasing Complexity of IT Infrastructure (Cloud, Hybrid, Multi-Cloud).** Modern IT environments involve intricate, distributed architectures (cloud, hybrid, microservices), making manual management unsustainable.

02 **Explosion of IT Operational Data (Logs, Metrics, Traces).** Servers, networks, applications, and security tools generate massive amounts of logs, metrics, and traces, overwhelming human analysis capabilities.

03 **Shortage of Skilled IT Operations Professionals.** There's a significant global shortage of experienced IT operations and security staff, driving the need for AI to augment existing workforces.

04 **Demand for Proactive & Predictive IT Management (Zero Downtime).** Organizations demand that IT systems remain operational 24/7 with minimal disruption; AI helps predict and prevent outages.

05 **Rapid Cloud Adoption & Distributed Environments.** Securing and managing complex cloud and hybrid environments requires AI for continuous monitoring, anomaly detection, and optimization.

06 **Sophistication of Cyber Threats & Need for AI Defense.** Cyber adversaries are constantly evolving their attack methods; AI is needed for sophisticated threat detection and response.

07 **Pressure for IT Cost Optimization & Efficiency.** Organizations seek to improve IT efficiency and reduce operational expenditure through AI-driven automation and optimization.

08 **Growth of Automation & DevOps Practices.** AI is crucial for automating routine IT tasks, integrating into CI/CD pipelines, and enabling faster software delivery.

09 **User Expectations for High Availability & Performance.** Users expect IT services to be always available and highly performant, driving investment in AI for proactive management.

10 **Aging IT Infrastructure & Legacy Systems.** AI offers tools for monitoring and optimizing older IT infrastructure, extending its life, and improving performance before costly replacements.

§ 05 VARIATION 5 SECTORS

Impact by sector

The headline figure is an average. Where you work changes the picture.

Network Administrators	AI for network traffic analysis, anomaly detection, predictive network failures, and automated configuration. Focus on network resilience and performance.
System Administrators (Server/OS focus)	AI for server performance monitoring, log analysis, automated patching, and predictive hardware failure. Focus on server health and stability.
Cloud Administrators	AI for cloud resource optimization, cost management, auto-scaling, and security posture management. Focus on cloud efficiency and compliance.
DevOps Engineers (Infrastructure Focus)	AI for automating infrastructure as code, CI/CD pipeline optimization, and integrating AI into monitoring tools. Focus on infrastructure automation and reliability.
IT Security Analysts (Operations Focus)	AI for alert correlation, threat hunting, and automated incident response in security operations. Focus on proactive threat detection and incident management.

§ 06 PREPARATION 8 SKILLS

Skills to build

The skills that keep the human part of this work valuable as the routine part is automated.

01 **AIOps Platform Proficiency.** Ability to effectively use, configure, and manage AIOps platforms for comprehensive IT monitoring, anomaly detection, and operational insights.

02 **Network & System Architecture Understanding.** Deep understanding of how various IT components (servers, networks, storage, applications) interoperate to form complex systems.

03 **Cybersecurity Fundamentals.** Knowledge of cyber threats, attack vectors, defensive strategies, and secure configuration principles for IT infrastructure.

04 **Automation & Scripting Skills.** Proficiency in scripting languages (e.g., Python, PowerShell) and automation tools (e.g., Ansible, Terraform) for automating routine IT tasks.

05 **Problem-Solving & Root Cause Analysis.** Ability to diagnose complex IT incidents, identify underlying causes, and develop effective solutions, often leveraging AI-provided data.

06 **Communication & Collaboration.** Clearly articulating complex technical issues, AI-driven insights, and remediation recommendations to technical and non-technical stakeholders.

07 **Cloud Computing Expertise.** Expertise in managing and optimizing IT infrastructure in cloud environments (AWS, Azure, GCP), including using AI for cost and resource optimization.

08 **Adaptability & Continuous Learning.** Willingness to learn new AI technologies, adapt IT workflows to evolving threats, and stay updated on the rapidly changing IT landscape.

§ 07 INSTRUMENTS 12 ENTRIES

Tools in use

KINDS OF TOOL WORTH KNOWING

01 **AIOps Platforms.** Platforms that use AI/ML to automate IT operations, detect anomalies, predict outages, and perform root cause analysis.

02 **Network Performance Monitoring (NPM) with AI.** Software that uses AI to analyze network traffic, identify performance bottlenecks, predict congestion, and detect security threats in network flow.

03 **Server Monitoring & APM (Application Performance Management) with AI.** Tools that monitor server health, resource utilization, and application performance, using AI to predict issues and optimize resource allocation.

04 **Cloud Management Platforms (CMP) with AI.** Platforms that provide centralized management and optimization of cloud resources, leveraging AI for cost control, security, and compliance.

05 **Security Information & Event Management (SIEM) with AI.** Platforms that aggregate security logs and alerts from across the IT environment and use AI/ML to detect advanced threats and anomalies.

06 **Generative AI for IT Documentation & Scripting.** Large Language Models (LLMs) used to assist in drafting system configurations, network diagrams, troubleshooting guides, or automation scripts.

NAMED TOOLS ALREADY IN USE

Dynatrace / Datadog / Splunk ITSI VISIT
Leading AIOps platforms that provide comprehensive observability, AI-powered root cause analysis, and automation capabilities across IT.

Cisco ThousandEyes / NetBrain (with automation) VISIT
Network monitoring solutions that are incorporating AI/ML for more intelligent alerting, traffic analysis, and performance optimization.

AppDynamics / New Relic / SolarWinds SAM (with AI) VISIT
Application Performance Monitoring (APM) tools that use AI to monitor and optimize application and server performance, predicting issues.

CloudHealth by VMware / Flexera One (with AI) VISIT
Cloud Management Platforms that leverage AI to provide insights into cloud costs, security posture, and resource optimization across multiple clouds.

Microsoft Sentinel / CrowdStrike Falcon Insight XDR / IBM QRadar VISIT

Leading SIEM and XDR platforms that integrate AI for user behavior analytics (UBA), anomaly detection, and automated threat investigation.

ChatGPT / Google Gemini (for IT documentation/scripting) VISIT

Generative AI models that can assist IT administrators in drafting technical documentation, configuration files, and automation scripts.

§ 08 EXAMPLES 5 EXAMPLES

In practice

Ways people in this role are already using AI, and what they get from it.

Automate Alert Correlation & Triage

EXAMPLE 1

HOW Implement an AI-driven AIOps platform that automatically ingests logs and metrics from all network devices and servers. The AI correlates related alerts, filters out noise, and prioritizes critical incidents, reducing manual alert fatigue for administrators.

GAIN Significantly reduces alert noise, speeds up incident identification, and allows administrators to focus on high-priority security and operational issues.

Predict Network Outages

EXAMPLE 2

HOW Deploy an AI model that analyzes historical network traffic patterns, device health metrics, and configuration changes. The AI predicts potential network congestion or hardware failures days in advance, allowing for proactive maintenance and preventing outages.

GAIN Minimizes costly downtime, enhances service reliability, and shifts IT operations from reactive firefighting to proactive maintenance.

Automate Patch Management

EXAMPLE 3

HOW Configure an AI-powered automation platform to autonomously identify servers and endpoints requiring patches, test patch compatibility, and deploy updates during off-peak hours. Administrators oversee the process and intervene for exceptions.

GAIN Ensures timely security updates, reduces manual effort in vulnerability management, and improves the overall security posture of IT infrastructure.

Generate IT Infrastructure Diagrams

EXAMPLE 4

HOW Provide a generative AI tool with details of a desired network topology or server configuration. The AI automatically generates initial network diagrams, architectural drawings, or configuration files for the administrator's review and refinement.

GAIN Accelerates documentation creation, ensures consistency in infrastructure representations, and streamlines communication for complex IT systems.

Proactively Detect Security Threats

EXAMPLE 5

HOW

Leverage an AI-powered SIEM (Security Information and Event Management) system that analyzes vast streams of security logs and user behavior. The AI identifies subtle anomalous activities or indicators of compromise, alerting administrators to potential security breaches before they escalate.

GAIN

Enhances threat detection capabilities, reduces false positives, and allows administrators to focus on investigating genuine security incidents, strengthening cyber defense.

§ 09 CONTEXT

How this role compares

Three neighbouring roles chosen to show the direction of travel.

Level 1 Help Desk Technicians (Basic, Scripted Support)

MORE EXPOSED

AI IMPACT

Very High (AI chatbots and automated knowledge bases can handle a large percentage of common L1 support queries and password resets.)

WORK MOVES TO

Role may contract or shift to managing/training AI support tools, handling chatbot escalations, or more complex L1 tasks.

AIOps Engineers / Site Reliability Engineers (SREs)

DIFFERENT SKILLS, GROWING

AI IMPACT

Foundational (They design, build, and implement the AI-driven IT operations and observability platforms.)

WORK MOVES TO

Deep skills in automation, cloud infrastructure, software engineering, data analysis, and AI/ML for IT operations.

IT Governance & Risk Managers (Strategic Policy Focus)

COMPLEMENTARY, LESS EXPOSED

AI IMPACT

Moderate Augmentation (AI assists in data collection for risk assessment and compliance reporting), but core focus is on defining IT policies, risk frameworks, and ensuring regulatory adherence, which is human-led.

WORK MOVES TO

Expertise in IT governance frameworks (COBIT, ITIL), risk assessment methodologies, regulatory compliance, and strategic policy development.

§ 10 VERDICT

Closing judgement

> For Network and Computer Systems Administrators, AI is not a replacement but a powerful force multiplier that will redefine their critical role. It automates the routine and amplifies their ability to monitor, troubleshoot, and secure complex IT infrastructure. The future administrator will be a master of human-AI teaming, blending their invaluable judgment, critical thinking, and strategic planning skills with AI's analytical power to ensure the most robust and resilient digital environments.

§ 11 BASIS REVISED 5 OCTOBER 2026

Evidence and revisions

What the exposure figure rests on, what changed when it was last revised, and the published work cited for this role.

SCORE

60 to 63

WINDOW

2-5 years (unchanged)

The 5 October 2026 review moved the score up by 3 points.

Exposure Index v2. Inputs: task applicability 51/100 (Microsoft AI applicability score 0.25 for Network and computer systems administrators); observed usage 45/100 (Anthropic observed exposure 0.34); official exposure tier 100/100 (BLS: very high); labour-market trajectory 60/100 (BLS projects employment to fall 4.1% over 2025–35); published adoption rating 70/100 (high adoption). Weighted base 63.2. Final score 63. The previous figure of 60 was raised by 3 points, a small change that comes from moving off scores rounded to the nearest five. The change window is unchanged.

HOW THE FIGURE IS BUILT (EXPOSURE INDEX V2)

Task applicability — Microsoft Research, AI applicability score	51 × 35%	17.7
Observed usage — Anthropic Economic Index, observed exposure	45 × 20%	9.0
Official exposure tier — US BLS AI-exposure category	100 × 20%	20.0
Labour-market trajectory — US BLS projected employment change 2025–35	60 × 10%	6.0
Published adoption rating — This report's adoption level	70 × 15%	10.5
Weighted base		63.2
Exposure score		63

MEASURES BEHIND THE SCORE

US Bureau of Labor Statistics · *Employment Projections 2025–35 and AI Exposure Categories* (27 August 2026)

AI-exposure tier: Very high. Projected employment change 2025–35: -4.1%. Matched to Network and computer systems administrators.

PUBLISHER PDF ARCHIVED COPY

Microsoft Research · *Working with AI: Measuring the Applicability of Generative AI to Occupations* (10 July 2025)

AI applicability score 0.25 (percentile 81 of 785 occupations) for SOC 15-1244.

PUBLISHER PDF ARCHIVED COPY

Anthropic · *Anthropic Economic Index report: Cadences* (26 June 2026)

Observed exposure 0.34 for SOC 15-1244 (percentile 93 of 756 occupations).

PUBLISHER PDF

UK Department for Science, Innovation and Technology · *Assessment of AI capabilities and the impact on the UK labour market* (28 January 2026)

UK context: around 70% of UK workers are in occupations with tasks AI could perform or enhance, above the US average; a one-standard-deviation rise in exposure was associated with a 3.9% fall in UK job postings.

PUBLISHER ARCHIVED COPY

Archived copies are served only where the licence permits; otherwise the link goes to the publisher. Full research library: https://www.careerguard.ai/sources

§ 12 APPENDIX

Method and sources

Each report was written from a large body of published research. The exposure score itself is computed, not written: it is the CareerGuard Exposure Index, a weighted average of occupation-level measures from the US Bureau of Labor Statistics (AI-exposure classification and 2025–35 projections), Microsoft Research (AI applicability scores) and Anthropic (observed exposure), together with the adoption rating published on the report. The organisations and publications below are the standing literature behind the narrative sections. Every source, with dates, licences and archived copies where we are permitted to hold them, is catalogued in the research library.

Exposure Index v2 (October 2026). Each input is scaled to 0–100 and weighted: task applicability 35% (Microsoft AI applicability score ÷ 0.5), observed usage 20% (Anthropic observed exposure ÷ 0.75), official exposure tier 20% (BLS very high = 100, high = 70, moderate = 40, low = 10), labour-market trajectory 10% (50 2.5 × projected % employment change), published adoption rating 15% (very high = 85, high = 70, medium-high = 55, medium = 40, low-medium = 25, low = 10). Inputs not measured for an occupation are dropped and the remaining weights renormalised. An editorial adjustment of at most ±12 points is allowed only for automation channels the measures cannot see (robotics, self-service, machine vision, medical imaging, RPA/OCR, generative video) and is always logged with its reason. Scores are whole numbers, not rounded to five. The change window shifts one notch (a year at each end) per ten points of movement.

I GLOBAL AND MACROECONOMIC IMPACT OF AI ON WORK

World Economic Forum

The Future of Jobs Report series — Employer survey of expected job growth and decline, skill shifts and technology adoption (2020, 2023 and 2025 editions); Artificial Intelligence and the Future of Entry-Level Work (2026).
AI governance and transformation reports — Frameworks on ethical AI, talent strategy and industry transformation.

McKinsey Global Institute
AI, Automation and the Future of Work series — Research quantifying automation potential by task, sector and demographic, from "Jobs Lost, Jobs Gained" to "Agents, robots, and us" (2025).
Industry-specific reports — Financial services, healthcare, manufacturing and others.

PwC
Global AI Jobs Barometer — Annual analysis of job postings and productivity by AI exposure (2024–2026 editions).
Upskilling Hopes and Fears survey — Employee perceptions and readiness.

Microsoft Research and Anthropic
Working with AI (2025); Anthropic Economic Index (2025–2026) — Occupation-level usage data from Copilot and Claude conversations, the two observed-usage measures behind the 2026 revision.

Stanford Digital Economy Lab and Stanford HAI
Canaries in the Coal Mine? (2025–2026); AI Index Report (annual) — Payroll evidence on early-career employment in exposed occupations; annual measurement of AI capability, investment and adoption.

Deloitte
Human Capital Trends series — Workforce, talent and HR technology trends.
Tech Trends series — Emerging technologies and their business implications.

Accenture
Technology Vision series — Forward-looking analysis of emerging technology, with emphasis on AI.
Fjord Trends — Design, innovation and human experience in a digital world.

Boston Consulting Group
AI/ML insights and industry solutions — "The AI Revolution in the Workplace" and related research.

EY
AI and workforce reports — Adoption, talent strategy and ethics.

IBM Institute for Business Value
AI and automation studies — Business models, workforce evolution and leadership.

OECD
AI Policy Observatory — International data and policy on AI, labour markets and skills.
Employment Outlook — Labour-market trends including technological impact (2023–2026 editions).

International Labour Organization
Generative AI and Jobs: A Refined Global Index of Occupational Exposure (2025) — Task-level exposure gradients for every ISCO occupation; successor to the 2023 global index.

International Monetary Fund
Staff Discussion Notes on AI and work (2024, 2026) — Complementarity framing: where AI augments and where it substitutes.

UK Department for Science, Innovation and Technology
Assessment of AI capabilities and the impact on the UK labour market (2026) — UK occupational exposure and job-posting evidence.

Brookings Institution
AI and automation research — Economic and social implications, displacement and skills.

Yale Budget Lab and Goldman Sachs Research
Tracking the Impact of AI on the Labor Market; AI and the US labour market (2026) — Aggregate labour-market monitoring; macro displacement estimates.

Oxford University (Oxford Martin School)
The Future of Employment — Frey & Osborne and subsequent research on susceptibility to automation.

MIT Technology Review
AI & Work — Reporting on AI research and its implications for industries and jobs.

Gartner
Hype Cycle for Artificial Intelligence — Maturity and adoption of AI technologies.
Future of Work reports — Workplace models and talent strategy.

U.S. Bureau of Labor Statistics
Employment Projections 2025–35; AI Exposure Categories; Occupational Outlook Handbook — Ten-year employment projections and, from the 2025 cycle, an AI-exposure tier for every detailed occupation.

Indeed Hiring Lab
AI at Work Report (2025) and posting-market updates — Skill-level transformation estimates and job-posting trends by occupation.

II CORE AI AND MACHINE-LEARNING RESEARCH

OpenAI
Research papers, blog and API documentation — Large language models, generative AI, safety and societal impact.

Google DeepMind
Research papers and blog — Reinforcement learning, AI for science, AGI and ethics.

Meta AI
Research papers and blog — Large language models, computer vision, AI for social good.

Hugging Face
Transformers library and model hub — Open-source state-of-the-art NLP models.

TensorFlow and PyTorch
Documentation and community forums — Core frameworks illustrating practical capability.

arXiv
cs.AI, cs.LG, cs.CV, cs.CL — Pre-print research.

NeurIPS and ICML
Conference proceedings — Top-tier academic research.

ACM and IEEE
Journals and proceedings — ACM Computing Surveys; IEEE Transactions on AI.

Kaggle
Datasets and competition solutions — Applied machine learning on real-world problems.

The Alan Turing Institute
Research and reports — Responsible and applied AI.

III ETHICAL AND RESPONSIBLE AI DEPLOYMENT

NIST
AI Risk Management Framework — Voluntary framework for managing AI risk.

European Commission
AI Act — Risk-tiered legal framework for AI.
Ethics Guidelines for Trustworthy AI — Principles for responsible development.

Partnership on AI
Research and best practice — Responsible AI development.

AI Now Institute
Annual reports — Social implications: power, inequality, rights.

ACM FAccT
Proceedings — Fairness, accountability and transparency.

Data & Society
Publications — Social implications of data-centric technology.

WIPO
Conversation on IP and AI — Intellectual-property implications of AI.

IEEE Global Initiative on Ethics of A/IS
Ethically Aligned Design — Recommendations for ethical AI design.

Center for AI and Digital Policy
Policy briefs — Accountable AI policy.