Source: https://transparency.oecd.ai/reports/ae49d6c8-1d3d-41af-98aa-340234445170

TELUS Digital: G7 Hiroshima AI Process (HAIP) Transparency Report

https://www.telusdigital.com/

Publication date: Jun 4, 2025, 12:22 PM PDT

Reporting period: 2025

Section 1 - Risk identification and evaluation

a. How does your organization define and/or classify different types of risks related to AI, such as unreasonable risks?

TELUS Digital has an AI Tool Inventory, where all tools involving AI are registered. Such Inventory is linked to a process where Information Security and Privacy aspects are also assessed. Privacy, Data & AI Governance then performs an assessment of the risks in line with the risk categories of the EU AI Act, based on the information provided by the business owner and other relevant stakeholders.

b. What practices does your organization use to identify and evaluate risks such as vulnerabilities, incidents, emerging risks and misuse, throughout the AI lifecycle?

TELUS Digital employs several practices to identify and evaluate risks such as vulnerabilities, incidents, emerging risks, and misuse throughout the AI lifecycle. These practices are part of a comprehensive approach to security and risk management. Here are the key practices:

Vulnerability Management:

- Vulnerability assessments and/or penetration testing are conducted quarterly or more frequently as warranted by the sensitivity and security requirements of the business process.
- Commercial products and/or services are used to assess all network subnets and servers hosting TELUS Digital information.
- Information about technical vulnerabilities is obtained in a timely fashion, and the organization's exposure to such vulnerabilities is evaluated.
- Appropriate measures are taken to address associated risks.

Risk Classification: TELUS Digital classifies vulnerabilities into different risk levels:

- Severe: Vulnerabilities related to malware/exploit/zero-day that have been confirmed to affect devices in TELUS Digital infrastructure.
- Critical: Vulnerabilities classified as critical due to their impact on the infrastructure or by recommendation of the vendor of the affected asset.
- High, Medium, and Low: Vulnerabilities classified based on their impact and vendor recommendations.

Incident Management:

- TELUS Digital has a Security Incident plan and procedures defined by the TI Information Security Committee (TISSC).
- The incident response process includes six stages: Preparation, Identification, Containment, Eradication, Recovery, and Follow-up.
- A record of incidents is maintained, including a description of the breach, time period, consequences, reporter's name, to whom it was reported, and data recovery procedures.

Regular Testing and Evaluation:

- Processes are in place for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.
- Penetration tests are undertaken at appropriate intervals to ensure the integrity and confidentiality of relevant systems.

AI-Specific Considerations: TELUS Digital's approach to risk management extends to AI systems.

- Applying the vulnerability management and incident response processes to AI systems and infrastructure.
- Conducting regular assessments of AI models for potential biases, security vulnerabilities, or misuse potential.
- Implementing monitoring systems to detect anomalies or unexpected behaviors in AI systems.

Compliance and Privacy:

- TELUS Digital ensures compliance with various data protection regulations, including GDPR, CCPA, PIPEDA, and others.
- Privacy impact assessments are conducted for data processed as controllers, ensuring that AI systems handling personal data are evaluated for privacy risks.

Continuous Improvement:

- The organization maintains up-to-date policies and frameworks that demonstrate accountability.
- Security programs are implemented with effective governance and management structures to protect data, including senior management oversight.

Third-Party Risk Management:

- TELUS Digital has processes in place to evaluate and manage risks associated with third-party service providers and subprocessors, which would extend to any AI-related services or components provided by external parties.

c. Describe how your organization conducts testing (e.g., red-teaming) to evaluate the model's/system's fitness for moving beyond the development stage?

TELUS Digital employs a comprehensive testing and evaluation framework to assess models/systems before moving them beyond the development stage. Here are the key practices:

Structured Testing Phase:

- A dedicated Software Quality Assurance and Testing Team conducts thorough testing in a separate environment from production
- Multiple testing methodologies are employed, including:
- Functional testing
- Integration testing
- End-to-end testing
- Acceptance testing
- Parallel testing
- Regression testing
- Stress testing
- String testing
- System testing
- Unit testing

Environment Separation and Controls:

- Strict separation between development/test and production environments
- Development and test systems are prohibited from running against operational databases
- Production data deemed confidential is prohibited in non-production environments unless specifically authorized
- Access controls enforce the separation between environments
- Separation of duties between personnel assigned to development/test and production environments

Quality Assurance Measures:

- Testing team employs functional tests to ensure:
- Expected functional requirements are met
- Security controls are present and operating properly
- Internal controls are functioning as intended
- Documentation of all corrections and modifications to maintain program integrity
- Validation of proper role-based access control (RBAC)

Security-Focused Testing:

- Testing of all security patches and system/software configuration changes before deployment
- Validation of:
- Input handling (to prevent cross-site scripting, injection flaws, malicious file execution)

- Error handling
- Secure cryptographic storage
- Secure communications
- Authentication mechanisms

Implementation Controls:

- Systems must pass acceptance criteria before moving to production
- Configuration and testing of system security parameters
- Parallel running of new and old systems to verify accuracy and reliability
- Post-implementation review to validate completion
- Documentation of any programming, procedural, or configuration changes made during the verification process

Change Management:

- All changes are controlled through a complete and robust configuration management process
- Changes must be approved and implemented in accordance with Change Management policy
- Analysis of potential security implications and possible risks
- Regular review and updates of configuration change control processes (at least yearly)

Continuous Evaluation:

- Regular testing, assessing, and evaluating the effectiveness of technical and organizational measures
- Testing the overall strength of defenses (technology, processes, and people) through simulated attacks
- Undertaking penetration tests at appropriate intervals to ensure system integrity and confidentiality

This comprehensive approach ensures that models and systems are thoroughly evaluated for functionality, security, and reliability before moving beyond the development stage. The process is designed to identify and address potential issues early in the development lifecycle while maintaining the separation between development and production environments to minimize risks.

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

Yes

e. Are quantitative and/or qualitative risk evaluation metrics used and if yes, with what caveats? Does your organization make vulnerability and incident reporting mechanisms accessible to a diverse set of stakeholders? Does your organization have incentive programs for the responsible disclosure of risks, incidents and vulnerabilities?

TELUS Digital employs a comprehensive approach to risk evaluation, vulnerability management, and incident reporting. Here's a breakdown of the practices:

Quantitative and Qualitative Risk Evaluation Metrics:

TELUS Digital uses both quantitative and qualitative metrics for risk evaluation:

- Employs an automated risk assessment matrix for change requests, which calculates risk based on factors such as urgency, impact, complexity, and confidence.
- Risk levels are categorized as Low (<=2.5 average), Moderate (>2.5 & < 3.5 average), and High (>=3.5 average).
- Vulnerabilities are classified into severity levels: Severe, Critical, High, Medium, and Low, based on their potential impact on the infrastructure and vendor recommendations.

Vulnerability and Incident Reporting Mechanisms:

TELUS Digital has established accessible reporting mechanisms for a diverse set of stakeholders:

- Employees can report incidents through an online form or by emailing TI.Privacy.Office@telusinternational.com.
- The reporting process requires detailed information about the incident, including circumstances, data compromised, discovery time, location, cause, and affected individuals.
- A documented process ensures appropriate people are involved in investigating and controlling the incident.
- The Security Investigations Team evaluates reported incidents and initiates appropriate protocols.
- There's a dedicated Security Investigations Team that issues reports on privacy incidents.

Incentive Programs for Responsible Disclosure:

The focus is on establishing clear reporting mechanisms and fostering a culture of security awareness rather than providing external incentives.

f. Is external independent expertise leveraged for the identification, assessment, and evaluation of risks and if yes, how? Does your organization have mechanisms to receive reports of risks, incidents or vulnerabilities by third parties?

TELUS Digital has a comprehensive approach to leveraging external expertise and managing third-party reporting mechanisms for risks and vulnerabilities:

External Independent Expertise:

TELUS Digital leverages external expertise in several ways:

- Annual audits by accredited trusted third parties following:
- ISO 27001 and ISO 27002 standards
- NIST 800-53 guidelines
- SSAE-18 Type II audits (when applicable)
- AICPA SysTrust audits (for non-financial services)
- External counsel involvement in:
- Risk assessments
- Incident response
- Legal due diligence
- Compliance evaluations
- Independent assurance reviews through:
- Internal Audit as the third line of defense
- External forensics investigators when required
- Regular vulnerability assessments and penetration testing by external parties

Third-Party Reporting Mechanisms:

TELUS Digital has established multiple channels for receiving reports of risks, incidents, or vulnerabilities:

- Formal incident reporting process through:
- Online reporting form
- Dedicated email channel (TI.Privacy.Office@telusinternational.com)
- Direct communication with the Privacy Office
- Service provider reporting requirements:
- Mandatory security incident response plans
- Immediate reporting of security breaches
- Regular status updates and attestations

Reporting Process Requirements:

For any incident report, the following information is required:

- Description of circumstances and individuals involved
- Details of compromised data

- Discovery time and location
- Cause of the incident
- Number and nature of affected individuals/organizations
- Immediate containment measures taken

Multi-Stakeholder Response Process:

The organization involves various stakeholders in the risk evaluation process:

- TI Security Investigations Team evaluates and reports on technical aspects
- Privacy Office assesses and initiates appropriate protocols
- External counsel provides legal guidance
- Communications team manages stakeholder communications
- Third-party forensics experts when needed

Documentation and Follow-up:

After receiving reports:

- Formal documentation of all incidents and responses
- Regular risk assessments (at least every two years or upon significant business changes)
- Post-incident analysis and lessons learned
- Updates to policies and procedures based on findings
- Regular audits to verify effectiveness of controls

Continuous Improvement:

The organization maintains:

- Regular updates to risk assessment methodologies
- Periodic review of reporting mechanisms
- Integration of lessons learned into future processes
- Training updates based on identified gaps
- Policy revisions based on audit findings

This comprehensive approach ensures that TELUS Digital not only leverages external expertise effectively but also maintains robust mechanisms for receiving and acting on reports from various stakeholders. The organization's multi-layered approach to risk management, combining internal controls with external validation and expertise, helps ensure comprehensive risk identification and mitigation.

g. Does your organization contribute to the development of and/or use international technical standards or best practices for the identification, assessment, and evaluation of risks?

TELUS Digital actively uses and implements international technical standards and best practices for risk identification, assessment, and evaluation, though the available documentation focuses more on implementation of standards rather than direct contributions to development:

Implementation of International Standards:

- ISO Standards:
- Follows ISO 27001 and ISO 27002 standards for information security management
- Uses these standards as the basis for audit methodology and compliance verification
- Maintains certification and updates policies to align with latest ISO standards (e.g., ISO 27001-2013)

Integration of Multiple Framework Standards:

- Implements a multi-framework approach by mapping controls across:
- NIST 800-53 Controls (updated to Version 5)
- HI Trust Framework
- PCI DSS Standards
- HIPAA Requirements
- ISO 27001 Controls

Best Practices Implementation:

- Incorporates industry best practices into various areas:
- Network security operations
- Application security (e.g., OWASP for web applications)
- Vulnerability assessment and remediation
- Security configuration management
- Risk assessment methodologies

Standards-Based Security Controls:

- Implements technical and organizational measures based on international standards:
- Continuous vulnerability assessment and remediation
- Security configuration management
- Access control systems
- Incident response protocols
- Data protection measures

Compliance and Verification:

- Regular audits by accredited third parties to verify compliance with:
- International standards
- Industry best practices

- Regulatory requirements
- SSAE-18 Type II audits when applicable
- AICPA SysTrust audits for specific scenarios

Documentation and Policy Alignment:

- Maintains documentation aligned with international standards
- Regular updates to policies and procedures to reflect changes in international standards
- Integration of standards into operational procedures and risk assessment methodologies

Risk Assessment Framework:

Uses standardized approaches for:

1. Vulnerability severity rating
2. Risk impact assessment
3. Security control implementation
4. Incident response procedures

h. How does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks, in particular systemic risks?

TELUS Digital employs a multi-faceted approach to collaborate with relevant stakeholders across sectors for assessing and adopting risk mitigation measures, including addressing systemic risks:

1. Cross-Sector Collaboration:

- TELUS Digital engages with various external parties, including legal counsel, forensic specialists, data breach resolution firms, and public relations experts.
- TELUS Digital establishes relationships with breach remediation vendors across different specialties, indicating a cross-sector approach to risk mitigation.

1. Stakeholder Engagement:

- The company involves multiple internal stakeholders in risk assessment and incident management, including the Privacy Office, Information Security Staff, IT Team, Law & Governance Team, and Operations/HR.
- External stakeholders such as customers, regulatory bodies, and law enforcement are also engaged when necessary.

1. Information Sharing:

- TELUS Digital has established protocols for sharing incident information with relevant parties, including affected individuals, media, privacy authorities, and other third parties like card issuers and banks.
- TELUS Digital maintains a centralized channel for reporting breaches, facilitating efficient information flow.

1. Collaborative Risk Assessment:

- The company conducts corruption risk assessments that consider factors such as the country of business, potential business partners, and the nature of proposed projects or transactions.
- This suggests a holistic approach to risk assessment that likely includes consideration of systemic risks.

1. Industry Standards and Best Practices:

- TELUS Digital adheres to international standards and best practices, implying participation in broader industry efforts to address common risks.
- They implement multiple framework standards, including ISO, NIST, HI Trust, PCI DSS, and HIPAA, which often address systemic risks within their respective domains.

1. Vendor Management:

- The company has a robust vendor management process, including due diligence checks and risk assessments of third parties.
- This approach helps mitigate systemic risks that might arise from the supply chain or partner ecosystems.

1. Continuous Improvement:

- TELUS Digital regularly updates its policies and procedures based on lessons learned from incidents, indicating an adaptive approach to risk management.
- They conduct post-incident reviews and formal audits, which likely contribute to identifying and addressing systemic risks.

1. Legal and Regulatory Compliance:

- The company collaborates with external counsel and regulatory bodies to ensure compliance with legal requirements, which often address systemic risks at an industry or national level.

1. Knowledge Sharing:

- TELUS Digital maintains relationships with outside counsel prior to incidents, suggesting ongoing dialogue and knowledge exchange about potential risks and mitigation strategies.

Section 2 - Risk management and information security

a. What steps does your organization take to address risks and vulnerabilities across the AI lifecycle?

TELUS Digital appears to have a comprehensive approach to addressing risks and vulnerabilities throughout the software development lifecycle, which extends to AI systems:

Development Phase:

- Incorporates information security throughout the software development life cycle.
- Implements coding standards, library controls, version controls, and software documentation.
- Ensures code review is performed by someone other than the original author.
- Implements proper role-based access control (RBAC).
- Perform Risk assessments based on the EU AI Act

Testing Phase:

- Conducts thorough testing in a separate environment from production.
- Employs functional tests to ensure expected functional, security, and internal controls are present and operating properly.
- Performs integration and end-to-end testing to verify components interact properly.
- Conducts acceptance tests to ensure systems meet defined acceptance criteria.
- Includes various types of testing.

Implementation Phase:

- Configures and tests system security parameters.
- Runs the new system in parallel with the old system to verify accuracy and reliability.
- Conducts post-implementation reviews to validate project completion and effectiveness.

Maintenance Phase:

- Ensures all changes are approved, documented, and disseminated.
- Addresses hardware and software configurations, operational standards, and procedures through change control.
- Administers patch management for technology-related changes.
- Establishes emergency controls and routine changes.

Continuous Security Measures:

- Implements continuous vulnerability assessment and remediation.
- Actively manages the security configuration of network infrastructure devices.
- Controls the use of administrative privileges.
- Maintains and monitors audit logs.
- Implements malware defenses and email/web browser protections.

Access Control and Monitoring:

- Implements controlled access based on the need-to-know principle.
- Actively manages the lifecycle of system and application accounts.
- Monitors and controls user identification and authorization.

Incident Response:

- Develops and implements an incident response infrastructure.
- Maintains a record of incidents, including description, time period, consequences, and reporting details.

Regular Evaluation:

- Conducts processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.
- Performs penetration tests and red team exercises at appropriate intervals.

Training and Skill Assessment:

- Identifies knowledge, skills, and abilities needed to support defense of the enterprise.
- Develops and executes plans to assess, identify, and remediate gaps through policy, organizational planning, training, and awareness programs.

Data Privacy and Protection:

- Implements measures for data portability and ensuring erasure/data retention.
- Uses encryption or functionally equivalent technology to protect data during transmission and storage.

b. How do testing measures inform actions to address identified risks?

TELUS Digital employs a comprehensive approach where testing measures directly inform actions to address identified risks. This process is integrated throughout security and development lifecycle. Here's how testing measures inform risk mitigation actions:

Continuous Vulnerability Assessment and Remediation:

- Continuously acquire, assess, and take action on new information to identify vulnerabilities.
- This ongoing process allows to remediate and minimizes the window of opportunity for attackers.
- The continuous nature ensures that newly discovered vulnerabilities are quickly addressed.

Severity-Based Risk Assessment:

- Vulnerabilities are classified into different severity levels: Severe, Critical, High, Medium, and Low.
- This classification is based on the potential impact on the infrastructure and vendor recommendations.
- The severity level directly informs the priority and urgency of remediation actions.

Automated Scanning and Reporting:

- Automated scanning tools are used to determine vulnerable servers, systems, and workstations.
- These tools provide lists of vulnerabilities and their severity.
- The automated nature allows for regular and consistent risk assessment.

Penetration Testing:

- Penetration tests are conducted at appropriate intervals to ensure the integrity and confidentiality of systems.
- These tests simulate real-world attack scenarios, providing insights into potential vulnerabilities that automated scans might miss.
- Results from these tests directly inform security improvements and risk mitigation strategies.

Regular Security Configuration Management:

- Actively manage, track, report on, and correct the security configuration of various systems.
- This process helps prevent attackers from exploiting vulnerable services and settings.
- Regular reviews and updates to configurations are informed by testing results.

Audit Log Analysis:

- Audit logs of events are collected, managed, and analyzed to detect, understand, or recover from attacks.
- Periodic verification of logs informs remediation efforts.
- This analysis helps in identifying patterns or anomalies that might indicate security risks.

Application Software Security:

- The security lifecycle of all in-house developed and acquired software is managed to prevent, detect, and correct security weaknesses.
- Testing during development and post-deployment informs necessary security improvements.

Incident Response Management:

- An incident response infrastructure is maintained, including plans, defined roles, and communication protocols.
- Records of incidents, including their description, time period, and consequences, are kept.
- This historical data informs future risk mitigation strategies and helps in identifying recurring issues.

Regular Effectiveness Evaluation:

- Processes are in place for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.
- These evaluations inform updates to security protocols and risk mitigation strategies.

Patch Management:

- A documented patch management program is maintained.
- Testing of security patches and configuration changes before deployment informs the patching process.
- This ensures that patches address vulnerabilities without introducing new risks.

Environment Separation:

- Development/test environments are separate from the production environment.
- This separation allows for thorough testing of changes before they are implemented in the production environment, reducing the risk of introducing vulnerabilities.

Compliance Verification:

- Regular audits are conducted to verify compliance with security requirements.
- These audits inform necessary adjustments to security measures and risk mitigation strategies.

c. When does testing take place in secure environments, if at all, and if it does, how?

TELUS Digital implements a comprehensive approach to secure testing throughout the development lifecycle. Here's an overview of when and how testing takes place in secure environments:

Separation of Environments:

- TELUS Digital maintains separate development/test and production environments.
- Access controls are in place to enforce the separation between these environments.
- This separation ensures that testing activities do not impact the production environment and that production data is protected.

Testing Before Production Deployment:

- All changes, including security patches and software configuration changes, are tested before being deployed into production.
- This pre-deployment testing helps identify potential issues or vulnerabilities before they can affect the live environment.

Secure Testing Procedures:

- Testing includes validation of various security aspects, such as:
- Input validation to prevent cross-site scripting, injection flaws, and malicious file execution
- Proper error handling
- Secure cryptographic storage
- Secure communications
- Proper role-based access control (RBAC)

Data Protection in Testing:

- Production data is not used for testing and development, or it is sanitized before use.
- If confidential production data must be used in non-production environments, access is restricted to authorized personnel based on job responsibilities.
- Test data and accounts are removed before production systems become active.

Continuous Vulnerability Assessment:

- TELUS Digital employs continuous vulnerability assessment and remediation processes.
- This ongoing testing allows for the identification and addressing of vulnerabilities throughout the system lifecycle.

Penetration Testing:

- Penetration tests are conducted at appropriate intervals to ensure the integrity and confidentiality of systems.
- These tests simulate real-world attack scenarios in a controlled environment.

System and Integration Testing:

- Various types of testing are performed

Security Configuration Testing:

- The initial configuration of systems or networks is documented, processed, tested, and approved in detail.
- All subsequent changes to components are controlled through a robust configuration management process.

Patch Testing:

- A documented patch management program is in place.
- Patches are tested in a controlled environment before being applied to production systems.

Post-Implementation Testing:

- After implementation, new systems are run in parallel with old systems to verify accuracy and reliability.
- Post-implementation reviews are conducted to validate project completion and effectiveness.

Regular Security Evaluations:

- Processes are in place for regularly testing, assessing, and evaluating the effectiveness of technical and organizational security measures.

Separation of Duties:

- Where possible, there is a separation of duties between personnel assigned to development/test environments and those assigned to the production environment.
- This separation helps maintain the integrity of the testing process and reduces the risk of unauthorized changes to production systems.

Secure Testing of Third-Party Components:

- For systems provided by third parties, TELUS Digital requires that these service providers undergo regular audits and provide attestation letters certifying compliance with security requirements.

Change Management in Testing:

- All changes made to information systems are controlled to preserve confidentiality, integrity, and availability.
- A configuration change control process is implemented at least yearly, ensuring that testing procedures remain up-to-date.

d. How does your organization promote data quality and mitigate risks of harmful bias, including in training and data collection processes?

TELUS Digital does not have specific policies on promoting data quality. However, we do have a AI Risk Management Policy and Standard, which addresses mitigating risks of harmful bias in AI systems:

Data Quality Assurance:

- TELUS Digital strives to keep personal data accurate and up-to-date, which is crucial for AI training data.
- Have processes in place for team members to update their personal information, suggesting a commitment to data accuracy.
- The company employs various safeguards, including administrative, physical, and technical security controls, which likely extend to maintaining data quality for AI systems.

Bias Mitigation:

- TELUS Digital promotes awareness of potential biases in data collection, particularly in areas like Equal Opportunity and Affirmative Action Records

Privacy by Design:

- The company has embraced Privacy by Design principles, striving to embed privacy-enhancing measures into all processes. This approach likely extends to AI development, helping to mitigate risks of harmful bias.

Data Minimization and Anonymization:

- TELUS Digital practices data minimization and anonymization/pseudonymization for various purposes, which can help reduce bias in AI training data.

Ethical Considerations:

- The company conducts ethics surveys, indicating a focus on ethical practices which likely extends to AI development.

Regular Assessments:

- TELUS Digital performs Data Protection Impact Assessments (DPIAs) when using innovative technologies like artificial intelligence, suggesting a proactive approach to identifying and mitigating risks.

Transparency and Accountability:

- Have appointed a Data Protection Officer to oversee data privacy compliance, which likely includes oversight of AI systems and data usage.

Training and Awareness:

- TELUS Digital takes privacy and security training seriously, which likely includes awareness of bias in data and AI systems.

Continuous Improvement:

- Regularly review and update policies to remain current with changing technologies and laws, suggesting an adaptive approach to managing AI-related risks.

Diverse Stakeholder Engagement:

- The company engages with various stakeholders, including team members and customers, which could help in identifying and addressing potential biases from different perspectives.

e. How does your organization protect intellectual property, including copyright-protected content?

TELUS Digital has a robust system in place to protect intellectual property and copyright-protected content. The approach is multi-faceted and includes the following key elements:

Information Classification System: TELUS Digital categorizes all information into four main classifications: a) Restricted: Highly sensitive and critical information b) Confidential: Important business information c) Proprietary: Default classification for all TELUS Digital-generated information d) Public: Information approved for public use

Data Labeling and Handling:

- All information assets are labeled based on sensitivity as 'Low', 'Medium', and 'High Risk'.
- Appropriate handling schemes are adopted for each label.

Access Control:

- Access to confidential information is restricted to TELUS Digital employees, contractors, and people with a business need to know.
- Logical and physical access controls are implemented to protect information assets.

Marking Guidelines:

- Confidential information is marked as "TELUS Digital's Confidential" or similar labels.
- Even unmarked information is presumed to be confidential unless expressly determined to be public.

Data Retention and Disposal:

- Specific retention periods are defined for different types of data (e.g., contracts, employee records).
- Secure disposal methods are used, including specially marked disposal bins and reliable erasure of electronic data.

Non-Disclosure and Confidentiality Agreements:

- Unauthorized reproduction or distribution of confidential documents is strictly prohibited.
- Violations are subject to sanctions as per confidentiality and non-disclosure agreements.

Proprietary Information Protection:

- Defined as confidential information known only to appropriate employees of the company.
- Includes measures to prevent unauthorized copying or removal from the company's operational control.

f. How does your organization protect privacy? How does your organization guard against systems divulging confidential or sensitive data?

TELUS Digital employs a comprehensive and multi-layered approach to protect privacy and prevent unauthorized disclosure of confidential or sensitive data. Here's an overview of the key strategies and measures:

Data Classification and Handling:

- Information is categorized into four main classifications: Restricted, Confidential, Proprietary, and Public.
- All information assets are labeled based on sensitivity as 'Low', 'Medium', and 'High Risk'.
- Appropriate handling schemes are adopted for each label and classification.

Access Control:

- Implements the principle of least privilege, allowing only authorized access necessary to complete assigned tasks.
- Access is restricted on a field-by-field basis, ensuring employees only have access to the data they need.
- Utilizes role-based access control (RBAC) for critical assets.
- Employs strong authentication mechanisms, including two-factor authentication.

Data Protection Measures:

- Implements encryption or functionally equivalent technology for data protection during transmission and storage.
- Prevents data exfiltration and mitigates the effects of exfiltrated data.
- Employs malware defenses and email/web browser protections to minimize attack surfaces.

Network Security:

- Utilizes firewalls, intrusion detection software, and other boundary defense mechanisms.
- Manages and controls network ports, protocols, and services to minimize vulnerabilities.
- Implements secure configurations for network devices such as firewalls, routers, and switches.

Monitoring and Auditing:

- Collects, manages, and analyzes audit logs to detect, understand, and recover from potential attacks.
- Actively manages the lifecycle of system and application accounts.
- Conducts continuous vulnerability assessments and remediation.

Privacy by Design:

- Embraces Privacy by Design principles, embedding privacy-enhancing measures into all processes.
- Implements data minimization and ensures data quality.

Employee Training and Awareness:

- Conducts security skills assessments and provides appropriate training.
- Raises awareness about privacy obligations and data protection responsibilities.

Incident Response:

- Maintains an incident response infrastructure with defined roles, training, and communication protocols.
- Records and manages security incidents, including breach descriptions and recovery procedures.

Regular Testing and Evaluation:

- Conducts regular penetration tests and simulates attacker actions to test defense strength.
- Continuously evaluates the effectiveness of technical and organizational security measures.

Data Retention and Destruction:

- Implements strict data retention policies aligned with legal and business requirements.
- Ensures secure disposal of data, including physical destruction of media when necessary.

Third-Party Management:

- Extends data protection requirements to vendors and third-party service providers.
- Conducts due diligence on third parties who may have access to sensitive data.

Compliance with Regulations:

- Adheres to various privacy regulations including PIPEDA, GDPR, HIPAA, and FCRA.
- Maintains a Data Privacy Policy that is reviewed at least annually.

Physical Security:

- Implements physical security measures such as access control, CCTV, and secure storage for hard copies of sensitive information.

Anonymization and Pseudonymization:

- Applies these techniques to protect individual privacy when processing data for analytics or long-term forecasting.

Governance:

- Appoints a Data Protection Officer to oversee data privacy compliance.
- Maintains a robust data security governance program with senior management oversight.

Contractual Protections:

- Uses confidentiality and non-disclosure agreements to legally bind individuals to protect sensitive information.

Penalties for Non-Compliance:

- Enforces strict penalties, including termination and potential legal action, for unauthorized disclosure of sensitive information.

g. How does your organization implement AI-specific information security practices pertaining to operational and cyber/physical security?

- **i. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?**
- **ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights? What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?**
- **iii. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?**
- **iv. How often are security measures reviewed?**
- **v. Does your organization have an insider threat detection program?**

TELUS Digital implements comprehensive security practices, including some that may apply to AI systems:

Vulnerability Management:

- Quarterly vulnerability assessments and penetration testing
- Classification of vulnerabilities (Severe, Critical, High, Medium, Low)
- Timely evaluation and remediation of vulnerabilities

Cybersecurity Measures:

- Industry-standard anti-virus software with real-time updates
- Documented patch management programs
- Strong network architecture with attack detection and traffic classification

IP and Trade Secret Protection:

- Principle of least privilege for data access
- Encryption for data in transit and storage
- Strict access controls based on business need

Secure Environment:

- Physical security measures (access cards, CCTV, secure storage)
- Secure configurations for hardware and software
- Regular testing and assessment of security measures

Incident Response:

- Six-stage response process: Preparation, Identification, Containment, Eradication, Recovery, Follow-up
- Immediate notification and real-time updates to clients

- Detailed incident reports and long-term solution implementation

Regular Reviews:

- Continuous evaluation of security measures
- Policy reviews to ensure relevance and compliance with changing laws

h. How does your organization address vulnerabilities, incidents, emerging risks?

TELUS Digital employs a comprehensive approach to managing vulnerabilities and risks across systems:

Continuous Monitoring:

- Quarterly vulnerability assessments
- Active monitoring tools for security breaches
- Real-time threat detection and classification

Incident Response:

- Six-stage response process (Preparation to Follow-up)
- Immediate notification and containment procedures
- Detailed incident documentation and solution implementation

Risk Management:

- Risk-based vulnerability classification (Severe to Low)
- Separation of production and non-production environments
- Regular security evaluations and updates

Post-Deployment:

- Continuous system monitoring
- Configuration change control process
- Regular assessment of security measures' effectiveness

Lifecycle Management:

- Documented change management procedures
- Data security throughout information lifecycle
- Regular updates and patch management

Section 3 - Transparency reporting on advanced AI systems

a. Does your organization publish clear and understandable reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems?

- **i. How often are such reports usually updated?**
- **ii. How are new significant releases reflected in such reports?**
- **iii. Which of the following information is included in your organization's publicly available documentation: details and results of the evaluations conducted for potential safety, security, and societal risks including risks to the enjoyment of human rights; assessments of the model's or system's effects and risks to safety and society (such as those related to harmful bias, discrimination, threats to protection of privacy or personal data, fairness); results of red-teaming or other testing conducted to evaluate the model's/system's fitness for moving beyond the development stage; capacities of a model/system and significant limitations in performance with implications for appropriate use domains; other technical documentation and instructions for use if relevant.**

TELUS Digital's security practices can be described as follows:

Comprehensive Security Approach:

- Multi-layered security for all systems, including AI
- Continuous vulnerability assessment and remediation
- Regular security testing and evaluation
- Data Protection Impact Assessments for innovative technologies like AI

Risk Assessment and Management:

- Ongoing vulnerability assessments
- Regular penetration testing
- Risk classification system (Severe, Critical, High, Medium, Low)

IP and Trade Secret Protection:

- Strict access controls (RBAC, need-to-know basis)
- Data classification system (Restricted, Confidential, Proprietary, Public)
- Encryption and secure storage practices

Vulnerability Management:

- Quarterly (minimum) vulnerability assessments
- Automated scanning and risk-based assessment
- Collaborative approach with vendors and partners

Security Reviews:

- Regular review cycles (quarterly, annual, continuous)
- Additional reviews triggered by system changes or new threats

Insider Threat Detection:

- Account monitoring and access control
- Behavioral analysis and activity logging

Additional Security Measures:

- Technical controls (encryption, network segmentation, firewalls)
- Administrative controls (training, policy enforcement)

Continuous Improvement:

- Regular assessment and updates to security measures
- Integration of lessons learned from incidents

b. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?

The approach to information sharing and stakeholder engagement is based on TELUS Digital’s general practices:

Incident Response and Communication:

- TELUS Digital has a structured incident response process that involves various internal stakeholders, including the Privacy Office, Information Security, Legal, and Operations teams.
- Established protocols for notifying internal stakeholders, including senior leadership and the Board of Directors, about privacy and security incidents.

External Communication:

- There are provisions for notifying external parties in case of privacy incidents, including affected individuals, media, privacy authorities, law enforcement, and other third parties when required.
- The company has established relationships with external counsel and vendors for incident response, suggesting some level of external collaboration.

Regulatory Compliance:

- TELUS Digital complies with various data protection regulations, which likely include requirements for reporting certain types of incidents or risks to regulatory bodies.

Risk Assessment Processes:

- The company conducts Data Protection Impact Assessments (DPIAs) for projects involving innovative technologies, including artificial intelligence.
- There's a structured approach to categorizing and assessing risks, which could potentially be applied to AI systems.

Transparency:

- There's evidence of a commitment to transparency, at least internally, with regular reporting and communication processes in place.

c. Does your organization disclose privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?

This is not applicable to our deployment of AI Systems.

d. Does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?

This is not applicable to our deployment of AI Systems.

e. Does your organization demonstrate transparency related to advanced AI systems through any other methods?

This is not applicable to our deployment of AI Systems.

Section 4 - Organizational governance, incident management and transparency

a. How has AI risk management been embedded in your organization governance framework? When and under what circumstances are policies updated?

TELUS Digital has embedded AI risk management into our organization's governance framework through a comprehensive approach:

1. AI Risk Management Policy and Standard: We have developed and implemented a dedicated AI Risk Management Policy and Standard. This policy provides a structured framework for identifying, assessing, and mitigating risks associated with AI systems throughout the lifecycle.
2. Integration with Global Risk Management Policy (GRMP): The AI Risk Management Policy and Standard is not standalone but is fully integrated into our broader Global Risk Management Policy (GRMP). This integration ensures that AI-specific risks are considered within the context of our overall risk management strategy.
3. Governance Structure: Our governance framework includes oversight from senior leadership, with clear roles and responsibilities defined for AI risk management. This may include an AI Ethics Committee or similar body responsible for reviewing high-risk AI projects.
4. Risk Assessment Process: We have established a systematic process for assessing AI-related risks, which is aligned with our overall risk assessment methodologies but tailored to address the unique challenges posed by AI systems.
5. Continuous Monitoring and Reporting: Our framework includes mechanisms for ongoing monitoring of AI systems in production, with regular reporting to relevant stakeholders on risk levels and mitigation efforts.

Policy Updates: Our AI Risk Management Policy and Standard, as part of the GRMP, is subject to regular reviews and updates. Policies are updated under the following circumstances:

1. Scheduled Reviews:
2. Annual reviews to ensure alignment with current best practices and technological advancements.
3. Comprehensive reviews every 2-3 years to reassess the entire framework.
4. Regulatory Changes: When new AI-related regulations or guidelines are introduced that impact our operations.
5. Incident Response: Following any significant AI-related incidents or near-misses, to incorporate lessons learned.
6. Technological Advancements: When new AI technologies or applications are adopted that may introduce novel risks.
7. Stakeholder Feedback: In response to feedback from internal teams, external auditors, or other relevant stakeholders.
8. Business Strategy Shifts: When there are significant changes in our business strategy or AI utilization.

9. Industry Developments: In response to emerging industry standards or best practices in AI risk management.

b. Are relevant staff trained on your organization’s governance policies and risk management practices? If so, how?

Yes, TELUS Digital has implemented a structured approach to training staff on governance policies and risk management practices. Here are the key aspects of the training program:

Training Program Structure:

1. Annual Privacy Training: All team members are required to complete a privacy refresher course on an annual basis to stay current with privacy and data protection obligations.
2. Role-Based Training: TELUS Digital has implemented a training and awareness program that addresses data privacy and data protection obligations specific to each role within the organization.

Key Training Areas:

Security and Risk Management:

- Training on the Global Security & Risk Policies
- Vulnerability management and risk assessment procedures
- Corporate device usage and security protocols
- Data protection and confidentiality requirements

Privacy Management:

- Training on privacy policies and procedures
- Understanding of various privacy regulations (PIPEDA, GDPR, HIPAA, FCRA)
- Data handling and protection protocols
- Incident reporting procedures

Governance and Compliance:

- Training on corporate policies and procedures
- Understanding of regulatory compliance obligations
- Security practices and protocols
- Change management procedures

Oversight and Accountability:

- The TI Privacy Office, headed by the Global Privacy Officer, manages privacy-related matters globally
- Training effectiveness is monitored and evaluated regularly
- Team members have access to resources and support through:
- Immediate managers
- HR prime

Team Member Privacy Office (TI.privacy.office@telusinternational.com)

c. Does your organization communicate its risk management policies and practices with users and/or the public? If so, how?

TELUS Digital has published a Customer Privacy Policy that outlines the responsibilities of the company and its subsidiaries concerning the protection of personal information entrusted to them by customers. This policy is publicly available on our website: https://www.telusDigital.com/privacypolicy

Confidentiality of Detailed Policies: It's important to note that while some information is made public, detailed security and risk management policies are kept confidential.

TELUS Digital has a comprehensive approach to communicating its risk management policies and practices to team members.

Team Member Privacy Policy: TELUS Digital has a detailed Team Member Privacy Policy that outlines how the company handles personal data, privacy expectations, and security practices. This policy is regularly updated and communicated to all team members.

Internal Communication Platforms: The company uses internal platforms to share information about policies and practices:

- Cosmos: An intranet where team members can access additional information about policies and practices.
- Company website: Some information is also available on the company's web pages.

Direct Communication Channels: Team members are encouraged to use various channels for inquiries about privacy and security practices:

- Immediate managers
- HR representatives
- Team Member Privacy Office (via email: TI.privacy.office@telusinternational.com)

TELUS Digital conducts regular training sessions and awareness programs to keep team members informed about risk management policies and practices.

d. Are steps taken to address reported incidents documented and maintained internally? If so, how?

TELUS Digital has implemented a robust system for documenting and maintaining steps taken to address reported incidents internally. Here's a summary of the approach:

1. Comprehensive Incident Documentation: When an incident is reported, detailed information is recorded, including the incident description, affected data, discovery time, location, cause, and impact on individuals or organizations.
2. Structured Response Process: The company follows a six-stage response process: Preparation, Identification, Containment, Eradication, Recovery, and Follow-up. This ensures a methodical approach to handling incidents.
3. Documentation Tools and Checklists: TELUS Digital utilizes various tools to maintain accurate records, including incident resolution checklists, a first 24 hours checklist, and a Privacy & Data Incident Reporting Form.
4. Post-Incident Reporting: After resolution, a detailed incident report is created, outlining the issues encountered, long-term preventive solutions, investigation results, and implemented remedial steps.
5. Clear Roles and Responsibilities: The process involves multiple teams with documented responsibilities, ensuring a coordinated response and clear accountability.
6. Incident Classification and Escalation: Incidents are classified using a severity matrix, and there's a documented escalation process to ensure appropriate handling based on the incident's impact.
7. Regular Maintenance and Review: The documentation process undergoes periodic reviews and updates to remain current and effective.
8. Comprehensive Communication Records: All internal and external communications related to an incident are documented, including updates to stakeholders and any required regulatory reporting.

This thorough documentation system helps TELUS Digital meet regulatory requirements, improve incident response processes, support training initiatives, prevent future incidents, demonstrate due diligence, and fulfill audit requirements. The process is designed to be comprehensive while maintaining the confidentiality and security of sensitive incident-related information.

e. How does your organization share relevant information about vulnerabilities, incidents, emerging risks, and misuse with others?

TELUS Digital has established a structured approach to sharing information about vulnerabilities, incidents, emerging risks, and misuse with different stakeholders.

Client Communication:

- Immediate notification through email when security breaches are discovered
- Establishment of a bridge for real-time client updates during incidents
- Detailed incident reports including:
- Description of issues encountered
- Long-term solutions implemented
- Preventive measures

Vulnerability Management and Reporting:

- Quarterly vulnerability assessments and penetration testing
- Classification system for vulnerabilities (Severe, Critical, High, Medium, Low)
- Timely evaluation and communication of system vulnerabilities
- Implementation of appropriate risk mitigation measures

Service Provider Communication:

- Annual audit reports from accredited third parties
- Regular monitoring and comparison of third-party services against Service Level Agreements
- Clear notification procedures for screening and security concerns
- Immediate reporting requirements for security breaches

Internal Stakeholder Communication:

- Regular updates to Senior Leadership Team (SLT)
- Communication through TELUScope (internal platform)
- Structured reporting channels through:
- Privacy Office
- Security team
- Information Technology team

Regulatory and Legal Communication:

- Compliance with industry and federal regulations
- Communication in accordance with legal requirements
- Prior notification and approval processes for sharing sensitive information
- Structured reporting to relevant authorities when required

Incident Response Communication:

- Network Operations Center manages immediate communications

- Establishment of communication bridges during incidents
- Creation of detailed incident reports
- Follow-up communications about implemented solutions

Privacy-Related Communication:

- All privacy-related incidents must be reported to the Privacy team before sharing with external parties
- Specific communication protocols for Customer Privacy Incidents
- Quarterly reports compiled by the TI Privacy Office

Public Communication: Limited to:

- Press releases
- Marketing brochures
- Announced performance and financial results
- Information posted on TELUS Digital's social network
- Job postings

Confidentiality Controls:

- Clear guidelines on what information can be shared externally
- Approval requirements from TELUS Digital Global Security & Risk team
- Protection of confidential information and intellectual property
- Strict controls on sharing sensitive security information

This structured approach ensures that:

- Relevant stakeholders receive timely and appropriate information
- Confidential information is protected
- Regulatory requirements are met
- Client trust is maintained
- Security risks are effectively communicated and managed
- Incident response is coordinated and effective

f. Does your organization share information, as appropriate, with relevant other stakeholders regarding advanced AI system incidents? If so, how? Does your organization share and report incident-related information publicly?

Not applicable, as TELUS Digital does not deploy Advanced AI systems.

g. How does your organization share research and best practices on addressing or managing risk?

TELUS Digital shares research and best practices on addressing and managing risk through several channels and methods:

1. Internal Documentation: The organization maintains comprehensive Global Security & Risk Policies, which are regularly updated (currently at Version 13 as of 2025). These policies likely serve as a repository of best practices and research findings.
2. Vulnerability Management: TELUS Digital conducts regular vulnerability assessments and penetration testing, sharing results and best practices internally to improve security measures.
3. Incident Reporting and Analysis: The company has a structured incident management process, which includes detailed reporting and analysis. Lessons learned from these incidents are likely shared to improve risk management practices.
4. Training and Awareness Programs: While not explicitly mentioned, it's common for organizations to use training programs to disseminate best practices and research findings on risk management.
5. Collaboration with External Parties: TELUS Digital works with service providers and undergoes third-party audits, which may involve sharing and receiving best practices on risk management.
6. Industry Standards Compliance: The organization adheres to industry standards like ISO 27001 and NIST 800-53 guidelines, which involves staying updated on and implementing best practices.
7. Client Communication: For client-related issues, TELUS Digital shares relevant information about risk management practices, tailored to specific client needs and contractual obligations.
8. Internal Committees: The existence of bodies like the TI Information Security Committee (TISSC) suggests that there are formal channels for sharing and discussing risk management strategies.
9. Confidentiality Controls: It's worth noting that TELUS Digital is cautious about sharing sensitive security information externally, indicating that most detailed research and best practices are likely shared internally or with select partners under confidentiality agreements.

h. Does your organization use international technical standards or best practices for AI risk management and governance policies?

TELUS Digital uses international technical standards and best practices for AI risk management and governance policies:

1. Have Privacy, Data and AI Governance Office, indicating a dedicated focus on AI governance.
2. Our practices align with international regulations like GDPR, CCPA, and PIPEDA.
3. Implement "data protection by design" and "data protection by default" principles.
4. Use Privacy by Design principles in our processes.
5. Have a team of Privacy Professionals globally covering legal requirements and best practices.
6. Conduct regular assessments and reviews of our privacy and security practices.

Section 5 - Content authentication & provenance mechanisms

a. What mechanisms, if any, does your organization put in place to allow users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?

Not applicable, as TELUS Digital does not deploy Advanced AI systems. TELUS Digital has in place:

1. A Privacy, Data and AI Governance Office, suggesting oversight of AI systems.
2. Specific policies for AI Community Contributors.
3. A commitment to transparency about data handling.
4. A practice of seeking consent for data use in certain situations.

b. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems? If yes, how? Does your organization use international technical standards or best practices when developing or implementing content provenance?

Not applicable, as TELUS Digital does not deploy Advanced AI systems. In any case, we implement transparency mechanisms to ensure that users are aware when they interacting with AI. Our product Fuel iX, is clearly labelled as an AI system and interactive tool.

Section 6 - Research & investment to advance AI safety & mitigate societal risks

a. How does your organization advance research and investment related to the following: security, safety, bias and disinformation, fairness, explainability and interpretability, transparency, robustness, and/or trustworthiness of advanced AI systems?

TELUS Digital advances research and investment in AI systems through several key initiatives and approaches:

Security and Safety:

- Implements robust data security governance programs
- Conducts regular vulnerability assessments and penetration testing
- Maintains comprehensive security controls and monitoring systems
- Uses AI tools for security verification and monitoring

Bias and Fairness:

- Embraces Privacy by Design principles
- Implements data minimization and quality controls
- Uses anonymization/pseudonymization techniques for analytics
- Ensures fair data processing practices

Transparency and Explainability:

- Maintains clear documentation of AI systems and processes
- Has a dedicated Privacy, Data and AI Governance Office
- Provides transparent policies and procedures
- Commits to being open about data handling practices

Robustness and Trustworthiness:

- Regular testing and evaluation of technical measures
- Continuous improvement of privacy and security programs
- Annual review of policies and procedures
- Implementation of industry best practices

Governance Structure:

- Has appointed Data Protection Officers globally
- Maintains a Privacy Program that undergoes continuous improvement
- Collaborates with Privacy Professionals across regions
- Regular assessment and updates of governance frameworks

Research Investment:

- Maintains an AI Community Contributors program
- Develops Data Annotation Solutions
- Invests in privacy-enhancing technologies
- Focuses on compliance with international standards

The organization emphasizes a balanced approach between innovation and responsible AI development

b. How does your organization collaborate on and invest in research to advance the state of content authentication and provenance?

TELUS Digital has the following practices in place for such purpose:

1. Implement robust data security governance programs and conduct regular audits.
2. Use advanced tools for security verification and monitoring.
3. Maintain comprehensive documentation of data flows and system configurations.
4. Collaborate with third-party auditors and service providers for security assessments.
5. Have a dedicated Privacy, Data and AI Governance Office, which may oversee related research initiatives.

c. Does your organization participate in projects, collaborations, and investments in research that support the advancement of AI safety, security, and trustworthiness, as well as risk evaluation and mitigation tools?

TELUS Digital demonstrates involvement in AI safety, security, and trustworthiness through several key areas:

Organizational Structure:

- Has dedicated TELUS Digital AI divisions across multiple countries
- Maintains a Privacy, Data and AI Governance Office
- Has established an AI Community Contributors program

Research and Development:

- Operates TELUS Digital Data Annotation Solutions
- Has specialized AI teams in multiple regions
- Develops AI tools like SAFE for security verification

Risk Management Tools:

- Implements vulnerability assessment and penetration testing
- Conducts regular risk evaluations
- Uses AI-powered monitoring and security tools

Collaborations:

- Works with international teams across multiple jurisdictions
- Partners with vendors and service providers for security testing
- Maintains relationships with privacy professionals globally

Security Standards:

- Adheres to international security frameworks (ISO 27001, NIST 800-53)
- Implements Privacy by Design principles
- Conducts regular security audits and assessments

d. What research or investment is your organization pursuing to minimize socio-economic and/or environmental risks from AI?

While specific research or investment in minimizing socio-economic and environmental risks from AI is not explicitly contemplates, TELUS Digital demonstrates awareness of AI-related risks through:

1. Global AI divisions across multiple countries, suggesting diverse perspectives on AI impact.
2. Implementation of Privacy by Design principles in processes.
3. A dedicated Privacy, Data and AI Governance Office overseeing AI-related matters.
4. Regular risk assessments and privacy impact analyses for data processing.
5. Compliance with various international data protection regulations.

Section 7 - Advancing human and global interests

a. What research or investment is your organization pursuing to maximize socio-economic and environmental benefits from AI? Please provide examples.

While specific research or investment in maximizing socio-economic and environmental benefits from AI is not explicitly detailed, TELUS Digital demonstrates some commitment to responsible AI development:

1. Global AI presence: TELUS Digital AI divisions operate in multiple countries, potentially contributing to local economies and knowledge sharing.
2. AI Community Contributors program: Engagement with a broader community in AI development.
3. Data Annotation Solutions: This initiative may create job opportunities and contribute to AI advancement.
4. Privacy and ethical considerations: TELUS Digital emphasizes privacy protection and ethical data use, which indirectly contributes to responsible AI development.
5. Health and wellbeing initiatives: While not AI-specific, TELUS Digital's focus on employee wellbeing informs the approach to AI's societal impact.

b. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities, limitations and impacts of advanced AI systems? Please provide examples.

While TELUS Digital doesn't explicitly include AI-specific digital literacy programs on our scope of training, we do emphasize:

1. Privacy and security training for team members
2. An AI Community Contributors program
3. Transparency about data handling and AI tool usage
4. General awareness initiatives about data protection and privacy

c. Does your organization prioritize AI projects for responsible stewardship of trustworthy and human-centric AI in support of the UN Sustainable Development Goals? Please provide examples.

Not at the moment.

d. Does your organization collaborate with civil society and community groups to identify and develop AI solutions in support of the UN Sustainable Development Goals and to address the world's greatest challenges? Please provide examples.

Not at the moment.