PRIVACY NOTICE FOR COMPANIES

PRIVACY NOTICE FOR COMPANIES

Comprehensive Data Protection and Personal Information Handling Framework

PART 1: INTRODUCTION AND CORE INFORMATION

1. PURPOSE AND LEGAL FRAMEWORK

1.1 Purpose of This Document

SM WEB SYSTEMS, a (PTY) LTD incorporated/registered under the laws of South Africa with registration number 2026/031662/07, located at 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094 (hereinafter referred to as "the Company," "we," "us," or "our"), is committed to protecting the privacy and security of your personal information.

This Privacy Notice describes how we collect, use, store, protect, and process personal information about you during and after your working relationship with us, or in the course of our business dealings with you.

1.2 Legal Compliance

This Privacy Notice complies with applicable data protection laws, including:

- Protection of Personal Information Act (POPIA), 4 of 2013 (South Africa)
- General Data Protection Regulation (GDPR) (EU) 2016/679 (if applicable)
- Consumer Protection Act (CPA), 68 of 2008 (South Africa)
- National Credit Act (NCA), 34 of 2005 (South Africa, if applicable)
- Other applicable provincial, national, or international data protection laws

1.3 Data Controller Status

The Company is a "Data Controller" under POPIA and GDPR. This means we are responsible for:

- Deciding how we collect and hold personal information about you
- Determining the purposes for processing your personal information
- Ensuring compliance with data protection obligations
- Protecting your rights regarding your personal information

- Notifying you of how we process your information

1.4 Scope and Application

This Privacy Notice applies to:

- Current and former employees (full-time, part-time, temporary, contract)
- Candidates for employment or engagement opportunities
- Contractors, freelancers, and independent service providers
- Workers and temporary staff affiliated with the Company
- Customers and clients of the Company
- Suppliers and vendors engaged by the Company
- Business partners and prospective business partners
- Website visitors and online users (for digital services)
- Any individual whose personal information the Company processes

This notice may be updated at any time. We will notify you of substantial changes via email or by posting an updated notice at our principal place of business.

1.5 Important Information

Please read this Privacy Notice carefully, together with any supplementary privacy notices provided when we collect or process your personal information. It is important that you understand:

- What personal information we collect
- How we use your information
- Who we share your information with
- How long we keep your information
- What rights you have regarding your information
- How to contact us about your information

PART 2: PERSONAL INFORMATION WE COLLECT

2. CATEGORIES OF PERSONAL INFORMATION

2.1 Definition of Personal Data

"Personal Data" or "Personal Information" means any information about an identifiable individual. It does not include data where the identity has been permanently removed (anonymous data) or data about organizations that cannot identify individuals.

2.2 Categories of Information We Collect

The Company collects, stores, uses, and processes the following categories of personal information:

A. IDENTITY AND CONTACT INFORMATION:

- Full name (first name, middle name, surname)
- Title/honorific (Mr., Mrs., Dr., Prof., etc.)
- Residential address (street address, city, province, postal code)
- Business/workplace address
- Telephone numbers (landline, mobile, business)
- Personal email addresses and business email addresses
- Alternative contact information for emergencies

B. DEMOGRAPHIC INFORMATION:

- Date of birth and age
- Gender/sex
- Marital status
- Information about dependents (children, spouses, partners)
- Nationality and citizenship status
- Race, ethnicity, or cultural background (where necessary for legal compliance)

C. IDENTIFICATION AND VERIFICATION:

- National ID number / Passport number / Identification document number
- Driving license or learner's permit number
- Employee or contractor identification number
- Copies of official identification documents (ID book, passport, driver's license)
- Copies of birth certificates, marriage certificates, divorce decrees
- Evidence of right to work in South Africa (visas, permits, immigration documentation)

D. EMPLOYMENT AND ENGAGEMENT INFORMATION:

- Details of current and previous employment/engagement
- Job title, position, role, and responsibility description
- Start date and end date (if applicable)
- Employment type (permanent, contract, temporary, part-time, full-time)

- Location of employment or workplace
- Department or team assignment
- Reporting line and manager information
- Recruitment information (CV, cover letter, application form, references)
- Right to work documentation and work verification

E. FINANCIAL AND COMPENSATION INFORMATION:

- Bank account details (account number, branch code, account holder name)
- Payroll records and salary information
- Tax identification number and tax status information
- National Insurance number
- Pension provider information and pension benefits
- Details of annual leave, sick leave, and other entitlements
- Benefits information (medical aid, group insurance, provident funds)
- Compensation history and salary review records
- Details of bonuses, commissions, or incentives
- Information about deductions and garnishments

F. PERFORMANCE AND CONDUCT INFORMATION:

- Performance reviews and appraisals
- Performance ratings and feedback
- Training records and development history
- Qualifications and certifications held
- Disciplinary records and warnings (if applicable)
- Grievance complaints and dispute records
- Misconduct investigations
- Attendance and punctuality records
- Exit interviews (if applicable)

G. HEALTH AND SAFETY INFORMATION:

- Medical conditions and health history (where relevant to employment)
- Health and sickness records (medical certificates, sick leave records)
- Disability information and reasonable accommodation requests
- Workplace injury records and incident reports
- Mental health information (if disclosed for support purposes)
- Vaccination status and health screening results (if mandatory for role)
- Occupational health assessment results
- Emergency contact information for medical purposes

H. SPECIAL CATEGORIES OF PERSONAL INFORMATION:

Also known as "sensitive" or "special" personal information requiring enhanced protection:

- Information about health (medical conditions, health history, disabilities)
- Information about race, ethnicity, or cultural background
- Information about religious or philosophical beliefs
- Information about trade union membership
- Information about political opinions or affiliations
- Genetic data (if collected through health screening)
- Biometric data (fingerprints, facial recognition, iris scans for security/access control)
- Data concerning sex life or sexual orientation (if voluntarily disclosed)

I. SECURITY AND SYSTEM MONITORING INFORMATION:

- Computer and device usage information
- Internet browsing history on Company systems
- Email communications (sent/received through Company systems)
- Access logs and authentication records
- CCTV footage (if recorded at workplace)
- Telephone call records (if recorded for quality/training purposes)
- Mobile device management information
- VPN and remote access logs
- Parking garage access records

J. FINANCIAL AND CREDIT INFORMATION (if applicable):

- Credit history and credit scores (if employment involves credit assessment)
- Banking information and financial records
- Criminal record (if relevant to position or legal requirement)
- Court orders and financial judgments
- Debt collection records (if applicable)

K. ONLINE AND DIGITAL INFORMATION (if you access Company digital services):

- IP address and device information
- Cookie identifiers and tracking information
- Login credentials and authentication data
- Website usage data and clickstream data
- Social media profile information (if provided by you)
- Electronic communication preferences
- Survey responses and feedback information

L. LOCATION INFORMATION:

- Workplace location and office/site assignment
- GPS/mobile location data (if using Company devices)
- Travel information and movement logs
- Home address and emergency contact address

M. PHOTOGRAPHS AND VIDEO:

- Employee photographs (for ID badges, directories, company communications)
- Video footage (from workplace CCTV, training videos, team recordings)
- Images from company events, training, or team activities

N. THIRD-PARTY PROVIDED INFORMATION:

- Information provided by references and referees
- Information from background checks or screening agencies
- Information from recruitment agencies or hiring partners
- Information from previous employers or educational institutions
- Information from social media or public sources (if relevant)

2.3 Information You Provide vs. Information We Collect

- Information you provide directly: CV, application form, questionnaires, conversations, emails, forms
- Information we collect from your work: Email records, access logs, performance reviews, timesheets
- Information from third parties: References, background check reports, recruitment agencies, credit bureaus
- Information from automated systems: IP addresses, login times, website usage, tracking cookies

PART 3: HOW WE COLLECT YOUR PERSONAL INFORMATION

3. SOURCES AND METHODS OF COLLECTION

3.1 Primary Collection Methods

A. RECRUITMENT AND APPLICATION PROCESS:

- Applications forms submitted by candidates
- Curriculum Vitae (CV) and Cover Letters

- Interview notes and assessment results
- Phone screenings and video interview recordings
- References and reference checks
- Background screening reports
- Recruitment agency submissions
- LinkedIn or other professional profile information

B. EMPLOYMENT AND ENGAGEMENT:

- Employment contracts and terms of engagement
- Onboarding forms and registration documents
- Tax forms (SARS forms, declaration forms)
- Bank account verification (for salary deposit)
- Pension and insurance declarations
- Emergency contact forms
- Health and safety questionnaires
- Training and development records
- Performance management forms

C. SYSTEMS AND AUTOMATED COLLECTION:

- Human Resource Management System (HRMS) records
- Time tracking and attendance systems
- Email and communication platforms
- Network access logs and IT systems
- CCTV and security systems
- Telephone systems (call recordings if applicable)
- Mobile device management systems
- Website cookies and analytics

D. THIRD-PARTY SOURCES:

- Background check and screening agencies
- Reference checks from previous employers
- Recruitment agencies and staffing partners
- Credit bureaus and financial institutions
- Public records and government databases
- Social media and online professional networks
- Insurance and benefits providers

3.2 Timing of Collection

During Application Phase:

- Personal contact information
- Educational and professional background
- Reference information
- Right to work documentation

During Onboarding:

- Identification and verification documents
- Bank account details
- Tax information
- Emergency contacts
- Health and safety information

During Employment/Engagement:

- Performance and conduct information
- Health and sickness records
- Disciplinary and grievance records
- Training and development records
- Continuous system-generated data (access logs, email records)

After Termination:

- Exit interview information
- Final benefit calculations
- Reference requests (from your future employers)

PART 4: HOW WE USE YOUR PERSONAL INFORMATION

4. LEGAL BASIS FOR PROCESSING

4.1 When We Can Use Your Information

The Company only processes personal information when the law allows us to do so. Under POPIA and GDPR, we process information based on one or more of the following legal bases:

A. CONTRACTUAL NECESSITY:

We need the information to perform our contract with you (employment contract, service agreement, etc.).

B. LEGAL OBLIGATION:

We need the information to comply with applicable laws (tax laws, labor laws, health and safety regulations, etc.).

C. LEGITIMATE INTERESTS:

We have a legitimate business interest in processing the information (protecting the Company, managing business operations, preventing fraud) that does not infringe your rights.

D. CONSENT:

You have given us explicit permission to process the information (usually for less common uses).

E. PROTECTION OF VITAL INTERESTS:

We need to process the information to protect your life or health or that of another person.

F. PUBLIC TASK:

Processing is necessary for us to perform a public function or exercise official authority.

G. EMPLOYMENT LAW PURPOSES:

We process information necessary for employment law, collective bargaining, or worker representation.

4.2 Specific Purposes for Processing

A. RECRUITMENT AND SELECTION:

- Making decisions about your application, interview, or appointment
- Conducting background checks and reference verification
- Assessing your qualifications and suitability for the position
- Checking your right to work in South Africa
- Communicating with candidates about job opportunities

B. CONTRACT PERFORMANCE AND EMPLOYMENT:

- Creating and maintaining your employment or engagement contract
- Managing and administering your employment relationship
- Providing you with work, assignments, and instructions

- Allocating roles, responsibilities, and project work
- Managing your schedule, shifts, and work location

C. COMPENSATION AND BENEFITS:

- Calculating and processing your salary, wages, or fees
- Managing deductions (tax, pension contributions, garnishments)
- Processing reimbursements and expense claims
- Managing benefits (medical aid, insurance, pension, provident fund)
- Handling leave applications and entitlements
- Processing annual reviews and salary adjustments

D. COMPLIANCE AND LEGAL OBLIGATIONS:

- Complying with tax laws and SARS requirements
- Reporting to government agencies and regulatory bodies
- Maintaining employment records as required by law
- Complying with industry-specific regulations
- Verifying right to work and work permits
- Maintaining required documentation for employment law

E. PAYROLL AND ACCOUNTING:

- Processing salaries, wages, and contractor fees
- Generating payslips and tax documentation
- Maintaining financial and accounting records
- Managing pension contributions and benefits
- Reconciling accounts and audits
- Preparing year-end tax returns (IRP5, IT3(a), etc.)

F. HEALTH, SAFETY, AND WELLBEING:

- Managing occupational health and safety obligations
- Responding to workplace accidents and incidents
- Managing workplace injuries and workers' compensation
- Providing employee wellness programs
- Conducting health and safety assessments
- Managing medical certificates for sick leave
- Responding to health emergencies

G. PERFORMANCE MANAGEMENT:

- Conducting performance reviews and appraisals
- Setting performance targets and goals
- Providing feedback and coaching

- Documenting performance concerns or issues
- Making promotion and advancement decisions
- Managing performance improvement plans

H. TRAINING AND DEVELOPMENT:

- Identifying training needs and development opportunities
- Delivering training programs and courses
- Recording certifications and qualifications
- Managing professional development plans
- Providing induction and onboarding

I. MANAGEMENT OF CONDUCT AND DISCIPLINE:

- Investigating misconduct or policy violations
- Conducting disciplinary hearings
- Documenting disciplinary action (warnings, suspension, termination)
- Managing grievance complaints and disputes
- Conducting workplace investigations
- Maintaining disciplinary records

J. TERMINATION AND EXIT:

- Managing resignation, retirement, or dismissal
- Calculating final payments and benefits
- Processing reference requests
- Conducting exit interviews
- Offboarding and returning Company property
- Maintaining post-employment records

K. LEGAL AND DISPUTE MANAGEMENT:

- Defending or pursuing legal claims
- Managing employment disputes and litigation
- Complying with subpoenas, court orders, or legal demands
- Gathering evidence for potential disputes
- Cooperating with regulatory investigations

L. BUSINESS MANAGEMENT AND PLANNING:

- Business planning and strategic decision-making
- Organizational planning and restructuring
- Budgeting and financial forecasting
- Data analysis and management reporting
- Mergers and acquisitions due diligence

- Succession planning

M. IT SYSTEMS AND SECURITY:

- Managing access to IT systems and networks
- Maintaining system security and preventing breaches
- Monitoring unauthorized access attempts
- System administration and troubleshooting
- Data backups and disaster recovery
- Cybersecurity and fraud prevention

N. WORKPLACE MONITORING AND COMPLIANCE:

- Monitoring business use of Company systems
- Ensuring compliance with IT policies and acceptable use policies
- Preventing data theft and intellectual property loss
- Monitoring for illegal activities or violations
- Recording phone calls and communications (where legally permitted)
- Video monitoring for security purposes

O. FRAUD PREVENTION AND SECURITY:

- Detecting and preventing fraud
- Conducting investigations into suspected fraud
- Protecting Company assets and property
- Preventing unauthorized access to systems
- Identifying false or misleading information
- Reporting suspected fraud to authorities

P. MARKETING AND COMMUNICATIONS (if applicable):

- Sending company newsletters and updates
- Communicating about company events and activities
- Sending promotional materials (only if you've consented)
- Gathering feedback on Company services
- Conducting employee surveys

Q. REFERENCE REQUESTS FROM FUTURE EMPLOYERS:

- Providing references at employee's request
- Confirming employment history and roles
- Commenting on performance and conduct
- Providing factual employment information

4.3 Overlapping Purposes

Some processing activities may have multiple legal bases. For example, calculating your salary is necessary for contract performance AND to comply with tax law (dual basis).

4.4 Information We Cannot Process Without

If you fail to provide certain information when requested, we may not be able to:

- Fully perform your employment contract
- Pay your salary or benefits correctly
- Comply with our legal obligations
- Provide you with employment or engagement
- Assess your suitability for the position

In such cases, the Company may decline to hire you, continue your employment, or complete your engagement.

4.5 Changes to Processing Purposes

We will only use your personal information for the purposes for which we collected it, unless:

- We reasonably consider that we need to use it for another compatible purpose, AND
- That purpose is compatible with the original purpose

If we need to use your information for an unrelated, new, or incompatible purpose, we will:

- Notify you in writing
- Explain the legal basis allowing the new use
- Give you the opportunity to object (if applicable)
- Seek new consent if required by law

PART 5: PROCESSING OF SPECIAL CATEGORIES OF INFORMATION

5. ENHANCED PROTECTIONS FOR SENSITIVE DATA

5.1 What Are Special Categories?

"Special Categories" of personal information (also called "sensitive" data) require higher levels of protection under POPIA and GDPR. These include:

- Information about health and medical conditions
- Information about race, ethnicity, or cultural background
- Information about religious or philosophical beliefs
- Information about trade union membership
- Information about political opinions or affiliations
- Genetic data
- Biometric data (fingerprints, facial recognition, iris scans)
- Data concerning sex life or sexual orientation
- Information about criminal convictions or offenses

5.2 When We Process Special Categories

We only process special categories of personal information when one or more of the following apply:

A. EMPLOYMENT LAW OBLIGATIONS:

- We must carry out our legal obligations in employment law
- We are exercising our employment-related legal rights
- We are exercising your employment-related legal rights
- Examples: Managing disability accommodation, processing medical certificates, complying with occupational health regulations

B. YOUR EXPLICIT CONSENT:

- You have given us clear, affirmative, informed consent
- Consent is specific to the type of information and purpose
- You can withdraw consent at any time
- Examples: Voluntary health screening, biometric access systems, shared health information for employee benefits

C. VITAL INTERESTS:

- Processing is necessary to protect your life, health, or safety
- Or the life, health, or safety of another person
- Examples: Medical emergency response, reporting workplace injuries

D. AUTHORIZED ACTIVITIES:

- We have authorization under applicable law to process special categories
- The processing is necessary for specific legal purposes

- Examples: Criminal record checks for certain positions, health and safety compliance

E. DATA MANIFESTLY MADE PUBLIC BY THE DATA SUBJECT:

- You have intentionally made the information public
- You have voluntarily disclosed it
- Example: Sharing disability information in your CV or during interview

5.3 Specific Uses of Special Categories

A. HEALTH AND MEDICAL INFORMATION:

- Managing workplace injuries and workers' compensation claims
- Responding to medical emergencies
- Arranging reasonable accommodations for disabilities
- Managing absence due to illness
- Processing medical certificates
- Managing employee wellness programs
- Occupational health assessments (where relevant to role)

B. DISABILITY INFORMATION:

- Making reasonable accommodations for disabled employees
- Assessing accessibility needs at the workplace
- Managing health and safety risks
- Determining suitable work assignments
- Accessing government disability support programs
- Ensuring workplace compliance with disability laws

C. BIOMETRIC DATA (if applicable):

- Security access control (fingerprint readers, facial recognition)
- Time and attendance tracking
- Secure computer access
- Secure facility access
- Identity verification

D. CRIMINAL RECORDS (if applicable):

- Conducting background checks for certain positions
- Assessing fit for positions requiring security clearance
- Complying with specific regulatory requirements
- Assessing suitability for working with vulnerable persons
- Assessing risk to Company security

5.4 Additional Safeguards for Special Categories

For special categories of information, we implement additional safeguards:

- Limited storage: Information is stored securely in limited locations
- Limited access: Only essential personnel can access the information
- Separate systems: Special categories may be stored in separate systems
- Enhanced encryption: Stronger encryption standards
- Regular audit: Regular audits of who accesses the information
- Minimization: Only the minimum information necessary is collected
- Purpose limitation: Strict limits on how the information is used

PART 6: DATA SHARING AND DISCLOSURE

6. WHO WE SHARE YOUR INFORMATION WITH

6.1 Third Parties We Disclose Information To

We may share your personal information with the following categories of third parties:

A. PAYROLL AND ACCOUNTING:

- Payroll service providers and processors
- Accountants and accounting firms
- Tax authorities (SARS)
- Pension and provident fund administrators
- Insurance companies (for benefits administration)
- Banks (for salary deposits and payments)

B. GOVERNMENT AND REGULATORY AGENCIES:

- Department of Labour
- SARS (for tax compliance)
- Unemployment Insurance Fund (UIF)
- CCMA (Commission for Conciliation, Mediation and Arbitration)
- Department of Home Affairs (for work permits/immigration)
- Health and safety regulatory bodies
- Industry-specific regulators
- Law enforcement (if legally required)

C. RECRUITMENT AND EMPLOYMENT AGENCIES:

- Recruitment agencies assisting with hiring
- Staffing agencies (for temporary workers)
- Outplacement services (if applicable)
- Headhunters and talent acquisition firms

D. SERVICE PROVIDERS AND VENDORS:

- IT service providers and cloud storage providers
- Human Resources management system providers
- Background check and screening companies
- Security and surveillance companies
- Telecommunications providers
- Office and facility management companies
- Training and development providers
- Employee assistance program (EAP) providers
- Occupational health service providers

E. PROFESSIONAL ADVISORS:

- Attorneys and law firms (for legal advice or representation)
- Auditors (internal and external)
- Management consultants
- Insurance brokers and advisors
- Financial advisors

F. BUSINESS PARTNERS AND CLIENTS:

- Affiliated companies or parent company
- Business partners for joint projects
- Clients of the Company (if you are representing us)
- Vendors and suppliers with whom you work

G. PROSPECTIVE ACQUIRERS:

- In case of merger, acquisition, or business sale
- Prospective acquirers and their advisors
- Transaction advisors

H. COURTS, LAW ENFORCEMENT, AND LEGAL PROCESSES:

- Courts and judges (if legally required)
- Law enforcement agencies (police, detective services)
- Data protection authorities
- Anti-corruption and anti-fraud agencies

I. VERIFICATION AND REFERENCE CHECKS:

- Previous employers (for reference checks)
- Educational institutions (to verify qualifications)
- Professional bodies (to verify certifications)
- Your future employers (if you request a reference)

6.2 Legal Basis for Sharing

We only share your information with third parties when:

- We have a contractual obligation to do so
- We are required by law to do so (mandatory disclosure)
- We have legitimate business interests that justify sharing
- You have given consent
- It is necessary to protect your or another's vital interests
- It is in the public interest

6.3 Data Protection Agreements

When we share information with third parties, we ensure:

- Third parties agree to protect your information with the same standard of protection we provide
- Third parties have adequate data security measures
- Third parties comply with applicable data protection laws
- Third parties use the information only for the purposes we specify
- Contracts include data protection clauses

6.4 Information We Do NOT Share Without Consent

We will NOT share the following without your consent (except if legally required):

- Medical or health information
- Biometric or genetic information
- Criminal record information
- Financial information beyond what's necessary
- Personal information for marketing by third parties

6.5 Conditions for Sharing

Third parties must:

- Be informed of the confidential nature of your information

- Use the information only for the specific purpose we specify
- Implement adequate security measures
- Not disclose the information to others without our permission
- Delete or return the information when no longer needed

PART 7: AUTOMATED DECISION-MAKING

7. AUTOMATED DECISIONS ABOUT YOU

7.1 What Is Automated Decision-Making?

Automated decision-making means making decisions about you based solely on automated processing of your information, without human involvement. This could include:

- Automated resume screening (AI-powered applicant tracking)
- Algorithmic performance scoring
- Automated disciplinary recommendations
- Automated promotion or progression suggestions
- Algorithmic salary comparisons
- Automated leave approval or denial

7.2 Your Protection

The Company will NOT subject you to automated decision-making that produces legal or other significant effects on you UNLESS:

- We have a lawful basis for doing so, AND
- We have given you prior notification, AND
- You have been given the opportunity to request human review

7.3 Right to Human Review

If we do use automated decision-making to make a significant decision about you, you have the right to:

- Request human review of the decision
- Obtain an explanation of how the decision was made
- Express your point of view
- Challenge the automated decision

7.4 How to Request Review

To request human review of an automated decision, contact:

- Email: userdata@smwebsystems.com or hr@smwebsystems.com
- Address: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Phone: +27670623697

PART 8: INTERNATIONAL DATA TRANSFERS

8. TRANSFERRING INFORMATION OUTSIDE SOUTH AFRICA

8.1 When We Transfer Information

The Company may, if necessary, transfer personal information we collect about you to recipients located outside South Africa, including:

- Parent companies or subsidiaries in other countries
- International service providers (cloud storage, software providers)
- Business partners in other jurisdictions
- Clients or customers in other countries
- Regulatory bodies in other jurisdictions

8.2 Protection During Transfer

To ensure your personal information receives adequate protection when transferred outside South Africa, we:

- Have assessed the data protection laws of the destination country
- Included appropriate data protection clauses in contracts with third parties
- Use encryption during transmission
- Use secure file transfer protocols
- Ensure adequate safeguards are in place
- May obtain your specific consent for certain transfers

8.3 EU/UK Data Transfers (if applicable)

If we transfer information to the European Union or United Kingdom, we rely on:

- Adequacy decisions (if the jurisdiction is recognized as having adequate protection)
- Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs)
- Your explicit consent (where required)

8.4 Your Rights

You have the right to be informed of:

- Destination country and jurisdiction
- Recipients in that jurisdiction
- Level of data protection in that jurisdiction
- Mechanisms we use to protect your information
- How to contact us regarding transfers

To inquire about data transfers, contact the Data Protection Officer at userdata@smwebsystems.com.

PART 9: DATA RETENTION

9. HOW LONG WE KEEP YOUR INFORMATION

9.1 Retention Principles

The Company retains personal information for only as long as necessary to fulfill the purposes for which we collected it, including:

- Satisfying legal obligations
- Meeting tax requirements
- Resolving disputes
- Enforcing contractual rights
- Maintaining business records

9.2 Specific Retention Periods

A. EMPLOYMENT RECORDS:

- Active employment: Duration of employment + 7 years after termination
- Reason: Tax compliance, labor law requirements, dispute resolution

B. PAYROLL AND FINANCIAL RECORDS:

- Payroll records: 7 years after last payment
- Reason: Tax compliance (SARS retention requirements), pension/UIF requirements
- Tax documentation: At least 5 years (SARS requirement)

C. HEALTH AND SAFETY RECORDS:

- Incident reports: 7 years after incident
- Medical records related to workplace: 10 years (occupational health requirement)
- Workers' compensation: 20 years (statutory requirement)

D. DISCIPLINARY AND PERFORMANCE RECORDS:

- Disciplinary records: 5 years after final resolution
- Performance reviews: 5 years after review date
- Grievance records: 5 years after resolution

E. RECRUITMENT RECORDS (unsuccessful candidates):

- Application materials: 6 months or until position is filled + 6 months
- Reason: To manage recruitment process and respond to inquiries

F. TRAINING AND DEVELOPMENT RECORDS:

- Training records: 5 years after training completion
- Certifications: Duration of validity + 5 years after expiry

G. TERMINATION DOCUMENTS:

- Exit documentation: 7 years after termination
- Final payslips and settlements: 7 years

H. LEGAL AND DISPUTE RECORDS:

- Litigation records: 7 years after case conclusion or settlement
- Subpoenas and court orders: As long as required by law

I. BACKGROUND CHECKS AND REFERENCE CHECKS:

- Retained: 3 years
- Reason: Future reference requirements and dispute resolution

J. CONTACT INFORMATION:

- After termination: May retain for administrative/legal purposes
- Recommended: Delete after 5 years unless legally required
- Exception: Can retain if you consent to stay on alumni or contact list

K. SYSTEM-GENERATED DATA (IT LOGS, ACCESS LOGS, EMAIL):

- Server logs and access records: 90 days to 2 years
- Email retention: Active + 2 years after deletion
- CCTV footage: 30 days unless incident occurred
- Backup copies: 6 months

9.3 How We Determine Retention Periods

To determine appropriate retention periods, we consider:

- Amount of data: Volume of personal information (large volumes may require longer review periods)
- Nature and sensitivity: Type of information (sensitive data may require longer retention for protection)
- Potential risks: Risk of harm from unauthorized disclosure (higher risk = longer retention)
- Processing purposes: How the information is used (legal/compliance uses may require longer retention)
- Alternative means: Whether we can achieve our purposes without retaining the data
- Legal requirements: Statutory retention periods (tax, labor, occupational health laws)
- Contractual obligations: Agreements requiring retention

9.4 Secure Deletion/Destruction

When we no longer need your personal information, we:

- Securely delete electronic information (permanent deletion, not just moving to trash)
- Shred or incinerate paper documents containing personal information
- Use secure data destruction methods that prevent recovery
- Ensure information cannot be reconstructed
- Confirm deletion through audit trails

9.5 Exceptions to Deletion

We may retain information beyond the normal retention period if:

- We have a legal obligation to retain it (court orders, statutory requirements)
- We have legitimate interests requiring retention (defense of claims)

- You have consented to retention
- We need it for a new compatible purpose

9.6 Information You May Request Retention Of

You may request that we retain your information for:

- Reference purposes
- Alumni network membership
- Future job opportunity notifications
- Continued communication about company events

Please contact the Data Protection Officer to request extended retention.

PART 10: INTERNATIONAL DATA PROTECTION STANDARDS

10. GDPR AND INTERNATIONAL COMPLIANCE

10.1 GDPR Compliance (if applicable)

If the Company processes the personal information of EU residents or has operations in the EU, we comply with the General Data Protection Regulation (GDPR), which requires:

- Lawful basis for processing (similar to POPIA)
- Data subject rights (access, correction, erasure, portability, objection)
- Data Protection Impact Assessments for high-risk processing
- Data Protection Officer designation
- Data breach notification within 72 hours
- Privacy by design and default

10.2 Additional GDPR Rights

Under GDPR, you may have additional rights including:

- Right to data portability: Receive your information in a portable, machine-readable format
- Right to object to automated decision-making (including profiling)
- Right to restrict processing
- Right to lodge complaints with data protection authorities

- Right to be informed in accessible language

10.3 Cross-Border Data Transfers

For transfers to non-adequacy countries, we use Standard Contractual Clauses (SCCs) or your explicit consent, and we:

- Conduct Transfer Impact Assessments
- Document data transfer mechanisms
- Ensure third parties implement appropriate safeguards

PART 11: YOUR RIGHTS

11. DATA SUBJECT RIGHTS AND HOW TO EXERCISE THEM

11.1 Overview of Your Rights

Under POPIA, GDPR, and other applicable data protection laws, you have rights regarding your personal information. These rights are explained below.

11.2 Right to Access Your Information

What is it?

You have the right to request access to personal information we hold about you. This is commonly called a "Data Subject Access Request" (DSAR) or "Access Request."

What does it include?

- Copy of the personal information we hold about you
- Details of what information we have
- How we are using your information
- Who we have shared it with
- How long we will retain it
- Your rights regarding the information

How to request:

- Email: userdata@smwebsystems.com and hr@smwebsystems.com

- Written request: Send to 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094, marked "Data Subject Access Request"
- In person: Visit our office during business hours
- Phone: +27670623697

How long it takes:

- South Africa (POPIA): 15 days to provide information (30 days in exceptional circumstances)
- EU (GDPR): 1 month (extendable to 3 months in complex cases)

Cost:

- No fee for providing your information
- We may charge a reasonable fee if your request is manifestly unfounded or excessive
- We will notify you of any fee before providing the information

What happens next:

- We will verify your identity
- We will gather your information
- We will provide a copy (electronic, printed, or other format as requested)
- We will explain the information if needed

11.3 Right to Correction (Right to Rectification)

What is it?

You have the right to ask us to correct or update personal information about you that is inaccurate, incomplete, or out of date.

What can you correct?

- Name or other identifying information if recorded incorrectly
- Contact details (address, phone number, email)
- Date of birth or other demographic information
- Employment details (job title, dates, department)
- Incorrect performance reviews or ratings
- Out-of-date qualification information
- Any other factual information that is wrong

How to request:

- Email: userdata@smwebsystems.com or hr@smwebsystems.com

- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Phone: +27670623697
- Conversation: Ask your manager or HR for correction

What happens:

- We will verify the incorrect information
- We will correct the information in our systems
- We will notify you when the correction is complete
- We may inform third parties who received the incorrect information

Limitations:

- If you dispute factual accuracy but we believe the information is correct, we may document your disagreement
- We cannot change subjective information (like performance ratings) unless they are manifestly unfair

11.4 Right to Erasure (Right to be Forgotten)

What is it?

You have the right to ask us to delete or remove personal information about you in certain circumstances.

When you can request deletion:

- The information is no longer necessary for the purpose we collected it
- You withdraw your consent (if consent was the legal basis)
- You object to the processing (if we're relying on legitimate interests)
- The information was unlawfully processed
- We must delete it to comply with legal obligations
- You request deletion as a child (under certain circumstances)

When we can refuse to delete:

- We need the information to perform a contract with you
- We need it to comply with legal obligations (tax, employment law)
- We need it to establish, exercise, or defend legal claims
- We have a legitimate interest in retaining it

How to request:

- Email: userdata@smwebsystems.com or hr@smwebsystems.com

- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Phone: +27670623697
- State clearly that you request deletion and your reason

Important:

- Deletion cannot be requested for:
    - Information we must retain by law (tax records, disciplinary records)
    - Information required for legal defense
    - Information related to ongoing disputes or litigation
    - Archived copies kept for legal record-keeping

11.5 Right to Object to Processing

What is it?

You have the right to object to our processing of your personal information in certain circumstances.

When you can object:

- We are processing your information based on legitimate interests and you have grounds to object
- We are sending you direct marketing or profiling related to marketing
- We are processing for research, statistics, or archiving
- We are using your information for a purpose you object to

When objection applies:

- Your circumstances are particular and warrant objection
- You have serious concerns about privacy or fairness
- Processing would cause you unwarranted harm

Important limitation:

- You CANNOT object to processing that is:
    - Necessary for contract performance (e.g., paying your salary)
    - Required by law
    - Necessary for a legal claim

How to object:

- Email: userdata@smwebsystems.com and hr@smwebsystems.com

- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Phone: +27670623697
- State clearly why you object and request cessation of processing

What happens:

- We will review your objection
- We will stop processing if your objection is valid
- We may explain why we cannot stop processing if we have legitimate grounds
- We will confirm in writing of our decision

11.6 Right to Restrict Processing

What is it?

You can ask us to suspend or limit how we use your personal information in certain situations.

When you can request restriction:

- You dispute the accuracy of the information (we won't delete it but we won't use it while we verify)
- The processing is unlawful and you oppose deletion
- We no longer need the information but you need it for legal claims
- You have objected to processing (while we consider your objection)

What restriction means:

- We can store your information but won't actively use it
- We won't share it with others (except with your consent or for legal requirements)
- We can still use it if you consent or for legal defense

How to request:

- Email: userdata@smwebsystems.com or hr@smwebsystems.com
- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- State clearly which information should be restricted and why

Duration:

- Restriction remains until the reason ends (e.g., accuracy verified, objection resolved)

11.7 Right to Data Portability

What is it?

You have the right to receive personal information about you in a structured, commonly used, machine-readable format (e.g., CSV, JSON, XML).

What can you request?

- Information you have provided to us
- Information we have collected about you
- In a portable format you can use elsewhere

When this applies:

- Processing is based on your consent or a contract with you
- It's technically feasible to provide in that format
- It doesn't infringe third parties' rights

How to request:

- Email: userdata@smwebsystems.com and hr@smwebsystems.com
- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Specify the format you want and where to send it

Important:

- Portability does NOT apply to all your information
- It doesn't apply to information we process for legal compliance
- Third-party assessments or subjective information may not be portable

11.8 Right to Withdraw Consent

What is it?

If we are processing your information based on your consent, you have the right to withdraw that consent at any time.

What counts as consent-based processing:

- Voluntary participation in wellness programs
- Consent to medical/health information sharing
- Voluntary participation in surveys or feedback
- Consent to additional data uses beyond job requirements

Important:

- Withdrawal of consent does NOT affect processing we did before you withdrew
- It may affect our ability to provide certain services (explain this when needed)
- Some processing may have other legal bases even without consent

How to withdraw consent:

- Email: userdata@smwebsystems.com or hr@smwebsystems.com
- Written request: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094
- Verbal request to your manager or HR
- Clearly state what consent you are withdrawing

What happens:

- We will stop processing based on that consent
- We will confirm in writing
- If other legal bases apply, we may continue processing
- We will explain what stops and what continues

11.9 Right to Appeal

What is it?

If you believe the Company has mishandled your personal information or violated your rights, you have the right to appeal our decision or lodge a complaint.

How to appeal within the Company:

1. Initial request: Contact the Data Protection Officer with your concern
2. Documentation: Provide details of what you believe is wrong
3. Review: The Data Protection Officer will review and respond within 30 days
4. Appeal: If unsatisfied, you can appeal to senior management

Right to lodge a complaint with authorities:

- South Africa (POPIA): Lodge a complaint with the Information Regulator
    - Website: www.inforegulator.org.za
    - Email: complaints@inforegulator.org.za
    - Address: Woodmead Office Park, 33 Woodmead Boulevard, Woodmead, 2191
- EU (GDPR): Lodge a complaint with your national Data Protection Authority
    - (Specific authority depends on country)

No penalty for lodging complaint:

- We will not punish, disadvantage, or retaliate against you for lodging a complaint
- Retaliation for reporting violations is illegal

11.10 How to Exercise Your Rights

Step 1: Submit Your Request

- Email the Data Protection Officer or use the contact method specified for your right
- Include your full name, employee ID (if applicable), and contact details
- Clearly state which right you are exercising
- Provide specific details (e.g., what information, time period, etc.)

Step 2: Identity Verification

- We will verify your identity to ensure we don't disclose to wrong person
- We may request:
    - Copy of ID
    - Signature confirmation
    - Answer to security questions
    - Other reasonable verification

Step 3: Process Your Request

- We will gather the requested information
- We will review applicable restrictions or limitations
- We will prepare our response

Step 4: Provide Response

- Timeframe: 15-30 days per law
- Format: As requested or as we determine appropriate
- In person, by email, by mail, or other method
- Include explanation of any restrictions on the right

Step 5: Appeal (if needed)

- If you disagree with our response, you can appeal to:
    - Senior management / Executive Director
    - Data Protection Officer
    - External authority (Information Regulator, data protection authority)

11.11 No Fee for Rights

You will not have to pay a fee to exercise your rights, unless:

- Your request is manifestly unfounded or excessive
- We charge a reasonable fee for additional copies
- You request a substantial amount of data requiring disproportionate effort

We will inform you of any fee before providing the information.

11.12 Responding to Your Rights

When you submit a request, we will:

- Acknowledge receipt within 5 business days
- Verify your identity appropriately
- Respond fully within the statutory timeframe
- Explain any reasons we cannot fully comply
- Advise you of your right to appeal or complain
- In no case, retaliate against you for exercising rights

PART 12: SECURITY MEASURES AND DATA PROTECTION

12. HOW WE PROTECT YOUR INFORMATION

12.1 Security Measures

The Company takes appropriate technical and organizational security measures to protect personal information, including:

A. TECHNICAL MEASURES:

- Encryption: AES-256 encryption for stored data; TLS 1.3 for transmitted data
- Access controls: Password-protected systems with strong authentication (multi-factor authentication where appropriate)
- Firewalls and intrusion detection: Network security to prevent unauthorized access
- Data backups: Regular encrypted backups stored in secure locations
- Secure disposal: Secure deletion of electronic data; shredding of paper documents
- Regular software updates: Timely patching of security vulnerabilities
- Network security: Firewalls, VPNs, secure remote access protocols

B. ORGANIZATIONAL MEASURES:

- Access restrictions: Only necessary personnel access personal information
- Employee training: Annual data security and privacy training for all staff
- Confidentiality agreements: All staff sign confidentiality and security obligations
- Role-based access: Different permission levels based on job function
- Audit trails: System logs of who accessed what information and when
- Incident response: Procedures to respond to suspected data breaches
- Data protection impact assessments: For high-risk processing activities
- Vendor management: Contractual requirements for third-party service providers

C. POLICY MEASURES:

- Acceptable Use Policy: Guidelines for appropriate use of information and systems
- Data Retention Policy: Clear policies on how long information is kept
- Breach Notification Policy: Procedures for responding to breaches
- Mobile Device Policy: Protection of information on mobile devices
- Remote Work Policy: Security requirements for offsite/remote access
- Third-party Management: Requirements for vendor security
- Whistleblower Protection: Safe channels to report security concerns

12.2 What Security Measures Do NOT Guarantee

While we maintain appropriate security, please understand:

- No system is 100% secure: Even with best efforts, breaches are possible
- Human error: Employees may inadvertently disclose information
- Viruses and malware: Despite precautions, cyber attacks may succeed
- Physical theft: Stored documents or devices may be stolen
- Insider threats: Employees may deliberately breach security

12.3 Your Role in Security

You have responsibilities to help protect your information:

- Keep credentials secure: Don't share passwords; use strong, unique passwords
- Report suspicious activity: Inform IT immediately of any security concerns
- Be cautious with email: Don't open suspicious attachments; don't click unknown links
- Lock your device: Always lock your computer when away from your desk

- Don't store sensitive data locally: Use Company systems for sensitive information
- Follow security policies: Comply with acceptable use and security policies
- Report incidents: Immediately report suspected breaches or unauthorized access

PART 13: DATA BREACHES AND BREACH NOTIFICATION

13. WHAT HAPPENS IF YOUR INFORMATION IS COMPROMISED

13.1 Definition of a Data Breach

A data breach occurs when personal information is accessed, used, or disclosed without authorization or authorization, such as:

- Unauthorized access to systems or databases
- Loss or theft of devices or documents containing personal information
- Accidental disclosure (sending to wrong recipient)
- Phishing attack resulting in credential compromise
- Malware or ransomware infection
- Insider breach or employee misconduct
- Third-party vendor breach

13.2 Our Breach Response Procedure

If a data breach occurs, we will:

Step 1: Immediate Response (within 24 hours)

- Isolate affected systems
- Stop the breach if ongoing
- Preserve evidence
- Notify internal incident response team
- Assess scope and severity

Step 2: Investigation (within 48-72 hours)

- Determine what information was accessed
- Identify affected individuals
- Determine cause of breach

- Assess risk to individuals
- Document breach details

Step 3: Notification to You (as required by law)

- If breach poses risk to your rights or interests
- Within timeframe required by law (typically within 15-30 days)
- By email or phone (using contact information on file)
- Include details of breach and risks

Step 4: Notification to Authorities

- Notify Information Regulator (if high risk and in South Africa)
- Notify other authorities if legally required

Step 5: Remediation

- Offer credit monitoring (if financial data breached)
- Provide identity theft protection
- Implement security improvements
- Provide guidance on protective measures you can take

13.3 Breach Notification Content

If we notify you of a breach, the notification will include:

- What information was involved
- Date/timeframe of the breach
- How the breach occurred
- Steps we have taken to respond
- Risks to you (e.g., identity theft risk)
- Steps we recommend you take (e.g., monitor credit, change passwords)
- Contact information for questions
- Our commitment to preventing future breaches

13.4 Exceptions to Notification

We do NOT have to notify you of breaches if:

- We determine the breach poses no real risk to you
- The information was encrypted and encryption key was not compromised
- We recovered the information before any unauthorized access
- We can demonstrate through forensic analysis that information was not accessed

13.5 Your Right to be Informed

You have the right to receive information about:

- Whether a breach occurred
- What information was involved
- Risks to you
- Steps we are taking to respond
- Steps you can take to protect yourself

13.6 Third-Party Breaches

If a third-party service provider we use has a breach affecting your information:

- We will investigate the breach
- We will determine if you are affected
- We will notify you if required
- We may terminate the relationship with the service provider
- We will enhance our vendor oversight

PART 14: CHANGES TO THIS PRIVACY NOTICE

14. UPDATES AND MODIFICATIONS

14.1 Right to Update

The Company reserves the right to update, modify, or supplement this Privacy Notice at any time to:

- Reflect changes to our data practices
- Comply with new legal requirements
- Clarify existing provisions
- Address new technologies or uses of data
- Improve transparency

14.2 How We Notify You

For substantial changes, we will:

- Email notification: Send updated notice to your email address on file

- Posted notice: Post updated notice at our principal place of business
- Online notification: If we maintain a website, post on the privacy page
- Individual notice: Provide written or in-person notice to affected individuals
- Request acknowledgment: May request your acknowledgment of the update

14.3 Timing of Changes

- Non-material changes: May take effect immediately
- Material changes: Generally give 30 days notice before changes take effect
- Changes required by law: May take effect immediately

14.4 Your Right Upon Update

If we make material changes you disagree with:

- You have the right to object (for certain types of processing)
- You may withdraw consent (if consent was the basis)
- You can request deletion (in some circumstances)
- You can file a complaint with the Information Regulator

14.5 Effective Date

This Privacy Notice was last updated on 2026-01-25.

Any revised version will have a new effective date at the top of the document.

PART 15: CONTACT INFORMATION

15. HOW TO CONTACT US

15.1 Data Protection Officer

For all privacy and data protection questions, requests, or concerns:

Name: Mukhtar Meer

Title: Data Protection Officer

Email: userdata@smwebsystems.com

Phone: +27670623697

Mailing Address: 122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094

Attn: Data Protection Officer

122 ROBERTS, AVENUE, KENSINGTON, GAUTENG, SOUTH AFRICA, 2094

Office Hours: Monday-Friday, 08:00-17:00

Response Time: We will acknowledge receipt within 5 business days and provide a full response within 30 days.

15.2 Alternative Contact Points

If you prefer to contact someone else:

Human Resources Department:

Email: hr@smwebsystems.com

Phone: +27670623697

Senior Management/Executive:

Email: mukhtar.meer@smwebsystems.com

Phone: +27670623697

15.3 Regulatory Authorities

To lodge a formal complaint about our handling of your personal information:

South Africa - Information Regulator (POPIA):

Website: www.inforegulator.org.za

Email: complaints@inforegulator.org.za

Postal Address: Information Regulator, Woodmead Office Park, 33 Woodmead, Boulevard, Woodmead, 2191,South Africa

EU - National Data Protection Authority (if applicable, varies by country)

Other Jurisdictions: Contact the relevant data protection authority for your location

15.4 When to Contact Us

Please contact us if:

- You have questions about this Privacy Notice
- You want to exercise any of your rights
- You believe your information has been misused
- You believe there is a data breach
- You want to lodge a complaint
- You want to provide feedback on our privacy practices
- You have data protection or privacy concerns

PART 16: ACKNOWLEDGMENT AND ACCEPTANCE

16. YOUR CONFIRMATION

By signing below or clicking "I Acknowledge," you confirm that:

- You have read and understood this Privacy Notice
- You understand what personal information we collect
- You understand how we use your information
- You understand who we share your information with
- You understand your rights regarding your information
- You understand the contact details for privacy questions
- You have had the opportunity to ask questions
- You have had the opportunity to seek independent legal advice
- You understand that this notice is subject to update
- You voluntarily agree to the processing described herein

SIGNATURE SECTION

For Employees, Contractors, and Workers:

I acknowledge and accept the Privacy Notice:

Printed Name: _____

Employee/Contractor ID (if applicable): _____

Email Address: _____

Signature: _____

Date: _____

For Parents/Guardians (if individual is under 18):

I acknowledge and accept the Privacy Notice on behalf of [MINOR'S NAME]:

Parent/Guardian Name: _____

Relationship to Minor: _____

Signature: _____

Date: _____

For Company Representative:

Accepted and authorized on behalf of [COMPANY NAME]:

Name: _____

Title: _____

Signature: _____

Date: _____

APPENDICES

APPENDIX A: GLOSSARY OF TERMS

Anonymous Data: Information that cannot identify an individual (permanently irreversibly anonymized).

Biometric Data: Unique physical/biological characteristics used for identification (fingerprints, facial recognition, iris scans).

Breach/Data Breach: Unauthorized access, use, disclosure, or loss of personal information.

Consent: Freely given, specific, informed, unambiguous indication of agreement to processing.

Controller: The entity that decides how and why personal information is processed (the Company).

Data Subject: The individual whose personal information is being processed.

Processing: Any operation on personal data (collection, use, sharing, storage, deletion, etc.).

Processor: Third party that processes personal information on behalf of the Controller.

Right to Work: Legal authorization to work in South Africa (permanent residence, visa, work permit, citizenship).

SARS: South African Revenue Service (tax authority).

Special Categories: Sensitive personal information (health, biometric, criminal, etc.).

UIF: Unemployment Insurance Fund (South African social security).

GDPR: General Data Protection Regulation (EU data protection law).

POPIA: Protection of Personal Information Act (South African data protection law).

Information Regulator: South African data protection authority.

APPENDIX B: SCHEDULE - SPECIFIC USES BY DEPARTMENT

HUMAN RESOURCES DEPARTMENT:

- Recruitment, selection, onboarding
- Payroll, benefits, leave management

- Performance management
- Disciplinary processes
- Workforce planning

FINANCE/ACCOUNTING:

- Salary processing
- Tax and statutory compliance
- Financial reporting
- Expense claims
- Pension administration

OPERATIONS/FACILITIES:

- Access control and security
- Workplace safety
- Facility management
- Equipment allocation

IT DEPARTMENT:

- System access and authentication
- Network security
- Data backup and recovery
- Cybersecurity incident response
- IT helpdesk support